PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-358707
(43)Date of publication of application : 26.12.2001

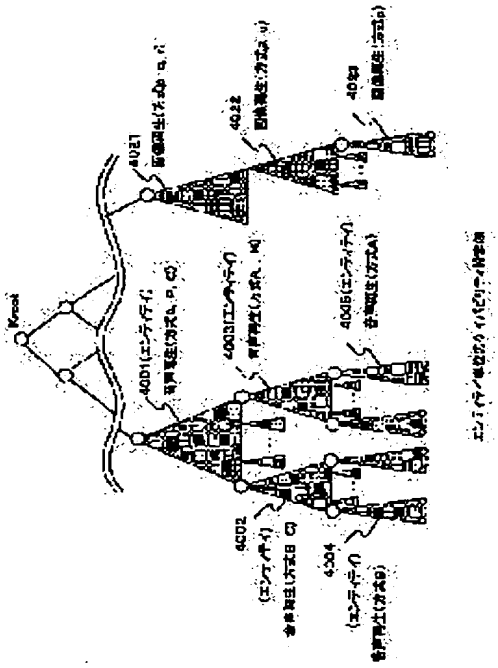
(51)Int.CI. H04L 9/10
G06F 12/00
G06F 12/14
G06F 13/00
G06F 15/00
H04L 9/08

(21)Application number : 2000-179693
(22)Date of filing : 15.06.2000

(71)Applicant : SONY CORP
(72)Inventor : KITATANI YOSHIMICHI
ISHIGURO RYUJI
OSAWA YOSHITOMO
ASANO TOMOYUKI

(54) INFORMATION PROCESSING SYSTEM AND METHOD USING CRYPTOGRAPHIC KEY BLOCK AND PROGRAM PROVIDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize an information processing system and method capable of generating and distributing an effective key block(EKB) in accordance with the data throughput of a device.
SOLUTION: In an entity which sets a subtree classified on the basis of capability as the data throughput of the device in a key tree obtained by making each key correspond to routes, nodes and leaves on paths from the root of the tree constructed with a plurality of devices as leaves, a sub effective key block(sub EKB) being effective in the entity is generated. In a key issuing center, the effective key block(EKB) that can be decoded only in an entity having common capability is generated on the basis of the capability information of the entity.



LEGAL STATUS

[Date of request for examination] 26.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－358707
（P2001－358707A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.'		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	9/10		Ｇ０６Ｆ	12/00	５３７Ｈ　５Ｂ０１７
Ｇ０６Ｆ	12/00	５３７		12/14	３２０Ｂ　５Ｂ０８２
	12/14	３２０		13/00	３５１Ｚ　５Ｂ０８５
	13/00	３５１		15/00	３３０Ｚ　５Ｂ０８９
	15/00	３３０	Ｈ０４Ｌ	9/00	６２１Ａ　５Ｊ１０４

審査請求　未請求　請求項の数21　ＯＬ　（全 50 頁）　最終頁に続く

(21)出願番号　特願2000－179693(P2000－179693)

(22)出願日　平成12年６月15日(2000.6.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　北谷　義道
東京都品川区北品川６丁目７番35号　ソニー株式会社内

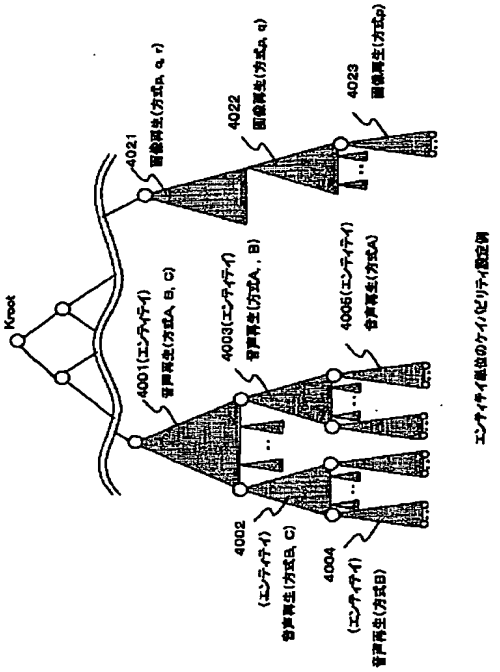
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　暗号鍵ブロックを用いた情報処理システムおよび情報処理方法、並びにプログラム提供媒体

(57)【要約】
【課題】　デバイスのデータ処理能力に応じて有効化キーブロック（ＥＫＢ）を生成して配信することを可能とした情報処理システムおよび方法を実現する。
【解決手段】　複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーに、デバイスのデータ処理能力としてのケイパビリティに基づいて区分したサブツリーを設定し、それぞれのサブツリーの管理主体であるエンティティにおいて、エンティティ内で有効なサブ有効化キーブロック（サブＥＫＢ）を生成し、キー発行センターにおいて、エンティティのケイパビリティ情報に基づいて、共通ケイパビリティを持つエンティティにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成する構成とした。



【特許請求の範囲】

【請求項１】複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する暗号鍵ブロックを用いた情報処理システムにおいて、

前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理し、該サブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成する複数のエンティテイと、

前記複数のエンティテイのケイパビリティ情報を管理し、共通のケイパビリティを持つエンティテイの生成するサブ有効化キーブロック（サブＥＫＢ）を用いて、共通のケイパビリティを持つエンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するキー発行センター（ＫＤＣ）と、

を有することを特徴とする暗号鍵ブロックを用いた情報処理システム。

【請求項２】前記キー発行センター（ＫＤＣ）は、

複数のエンティテイ各々の識別子と、エンティテイ各々のケイパビリティ情報と、エンティテイ各々のサブ有効化キーブロック（サブＥＫＢ）情報とを対応付けたケイパビリティ管理テーブルを有し、該ケイパビリティ管理テーブルに基づいて、デバイスに対する配信データの処理可能なエンティテイを選択して、該選択エンティテイ配下のデバイスでのみ復号可能な有効化キーブロック（ＥＫＢ）を生成する構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項３】前記キーツリーに対する新規追加エンティテイは、

該新規エンティテイ内のサブツリー内のノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成し、前記キー発行センター（ＫＤＣ）に対するサブＥＫＢの登録処理を実行するとともに、自己のエンティテイのケイパビリティ情報の通知処理を実行する構成であることを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項４】前記複数のエンティテイは、

１つのエンティテイの最下段の末端ノードを他のエンティテイの頂点ノード（サブルート）として構成した上位エンティテイおよび下位エンティテイの階層化構造を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項５】前記複数のエンティテイの各々は、

自己のエンティテイに属するサブツリーを構成するノードまたはリーフに対応するキーの設定、更新処理権限を有する構成であることを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項６】前記複数のエンティテイ中、エンティテイ内の最下段リーフを個々のデバイスに対応するリーフとした最下層のエンティテイに属するデバイスの各々は、

自己の属するエンティテイの頂点ノード（サブルート）から自己のデバイスに対応するリーフに至るパス上のノード、リーフに設定されたノードキーおよびリーフキーを格納した構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項７】前記複数のエンティテイの各々は、

自己のエンティテイの下位に、さらに自己管理エンティテイを追加するため、自己のエンティテイ内の最下段のノードまたはリーフ中の１以上のノードまたはリーフをリザーブノードとして保留して設定した構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項８】新規エンティテイを末端ノードに追加する上位エンティテイは、

新規エンティテイのサブツリーを設定するノードである上位エンティテイ末端ノードに対応するキーを、前記新規エンティテイの頂点ノード（サブルート）キーとして設定する構成であることを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項９】デバイスのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・デバイスに対応するリーフに至るパス上のノードに設定されたノードキーを更新し、更新ノードキーをリボークデバイス以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボークデバイスからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、デバイスのリボーク処理を実行する構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項１０】下位エンティテイのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・エンティテイに対応する末端ノードに至るパス上のノードに設定されたノードキーを

更新した更新サブＥＫＢを生成して上位エンティティに送信し、上位エンティティは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティティに送信し、最上位エンティティまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティティからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティティ単位のリボーク処理を実行する構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項１１】下位エンティティのリボーク処理を実行するエンティティは、エンティティ内の頂点ノード（サブルート）からリボーク・エンティティに対応する末端ノードに至るパス上の、該末端ノードを除くノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティティに送信し、上位エンティティは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティティに送信し、最上位エンティティまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティティからルートに至るパス上のリボーク・エンティティに対応する末端ノードを除くノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティティ単位のリボーク処理を実行する構成を有することを特徴とする請求項１に記載の暗号鍵ブロックを用いた情報処理システム。

【請求項１２】複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する情報処理システムにおける暗号鍵ブロックを用いた情報処理方法において、

前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理するエンティティにおいて、各エンティティのサブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成するステップと、

前記複数のエンティティのケイパビリティ情報を保有するキー発行センター（ＫＤＣ）において、前記複数のエンティティのケイパビリティ情報に基づいて、共通のケイパビリティを持つエンティティの生成するサブ有効化キーブロック（サブＥＫＢ）を抽出し共通のケイパビリティを持つエンティティにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップと、

を有することを特徴とする暗号鍵ブロックを用いた情報処理方法。

【請求項１３】前記キー発行センター（ＫＤＣ）における有効化キーブロック（ＥＫＢ）生成ステップは、

共通のケイパビリティを持つエンティティを選択するエンティティ選択ステップと、

前記エンティティ選択ステップにおいて選択されたエンティティによって構成されるエンティティ・ツリーを生成するステップと、

前記エンティティ・ツリーを構成するノードキーを更新するノードキー更新ステップと、

前記ノードキー更新ステップにおいて更新したノードキー、および選択エンティティのサブＥＫＢに基づいて選択エンティティにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップと、

を含むことを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１４】前記情報処理方法において、さらに、

前記キー発行センター（ＫＤＣ）は、

複数のエンティティ各々の識別子と、エンティティ各々のケイパビリティ情報と、エンティティ各々のサブ有効化キーブロック（サブＥＫＢ）情報とを対応付けたケイパビリティ管理テーブルを有し、該ケイパビリティ管理テーブルに基づいて、デバイスに対する配信データの処理可能なエンティティを選択して、該選択エンティティ配下のデバイスでのみ復号可能な有効化キーブロック（ＥＫＢ）を生成することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１５】前記情報処理方法において、さらに、

前記キーツリーに対する新規追加エンティティは、

該新規エンティティ内のサブツリー内のノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成し、前記キー発行センター（ＫＤＣ）に対するサブＥＫＢの登録処理を実行するとともに、自己のエンティティのケイパビリティ情報の通知処理を実行することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１６】前記情報処理方法において、さらに、

前記複数のエンティティの各々は、

自己のエンティティに属するサブツリーを構成するノードまたはリーフに対応するキーの設定、更新処理を実行することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１７】前記情報処理方法において、さらに、

新規エンティティを末端ノードに追加する上位エンティティは、

新規エンティティのサブツリーを設定するノードである

上位エンティティ末端ノードに対応するキーを、前記新規エンティティの頂点ノード（サブルート）キーとして設定することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１８】デバイスのリボーク処理を実行するエンティティは、エンティティ内の頂点ノード（サブルート）からリボーク・デバイスに対応するリーフに至るパス上のノードに設定されたノードキーを更新し、更新ノードキーをリボークデバイス以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成した更新サブＥＫＢを生成して上位エンティティに送信し、上位エンティティは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティティに送信し、最上位エンティティまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボークデバイスからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、デバイスのリボーク処理を実行することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項１９】下位エンティティのリボーク処理を実行するエンティティは、エンティティ内の頂点ノード（サブルート）からリボーク・エンティティに対応する末端ノードに至るパス上のノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティティに送信し、上位エンティティは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティティに送信し、最上位エンティティまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティティからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティティ単位のリボーク処理を実行することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項２０】下位エンティティのリボーク処理を実行するエンティティは、エンティティ内の頂点ノード（サブルート）からリボーク・エンティティに対応する末端ノードに至るパス上の、該末端ノードを除くノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティティに送信し、上位エンティティは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティティに送信し、最上位エンティティまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティティからルートに至るパス上のリボーク・エンティティに対応する末端ノードを除くノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティティ単位のリボーク処理を実行することを特徴とする請求項１２に記載の暗号鍵ブロックを用いた情報処理方法。

【請求項２１】複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する情報処理システムにおける有効化キーブロック（ＥＫＢ）生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理するエンティティにおいて、各エンティティのサブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成するステップと、

前記複数のエンティティのケイパビリティ情報を保有するキー発行センター（ＫＤＣ）において、前記複数のエンティティのケイパビリティ情報に基づいて、共通のケイパビリティを持つエンティティの生成するサブ有効化キーブロック（サブＥＫＢ）を抽出し共通のケイパビリティを持つエンティティにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップと、

を含むことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号鍵ブロックを用いた情報処理システムおよび情報処理方法、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステムおよび方法に関する。特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、例えばコンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とするとともに、階層的鍵配信ツリーを管理下のデバイスのデータ処理能力としてのケイパビリティに基づいて区分したサブツリーとしてのエンティティで管理する構成としてケイパビリティに基づく鍵配信および管理構成を実現した暗号鍵ブロックを用いた情報処理システムおよび情報処理方法、並びにプログラム提供媒体に関する。

【０００２】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはＰＣ等のに付属する記録再生機器内の記録デバイス、例えばメモリカード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

【０００３】ビデオゲーム機器、ＰＣ等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはＤＶＤ、ＣＤ等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるＲＡＭ、ＲＯＭ等を有する。

【０００４】音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００５】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００６】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【０００７】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００８】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Deta encryption standard）がある。

【０００９】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【００１０】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【００１１】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはＤＶＤ、ＣＤ等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

【００１２】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行なう。認証方式

には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通な鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

【００１３】本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とするとともに、階層的鍵配信ツリーを管理下のデバイスのデータ処理能力としてのケイパビリティに基づいて区分したサブツリーとしてのエンティテイで管理する構成としてケイパビリティに基づく鍵配信および管理構成を実現した暗号鍵ブロックを用いた情報処理システムおよび情報処理方法、並びにプログラム提供媒体を提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明の第１の側面は、複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する暗号鍵ブロックを用いた情報処理システムにおいて、前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理し、該サブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成する複数のエンティテイと、前記複数のエンティテイのケイパビリティ情報を管理し、共通のケイパビリティを持つエンティテイの生成するサブ有効化キーブロック（サブＥＫＢ）を用いて、共通のケイパビリティを持つエンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するキー発行センター（ＫＤＣ）と、を有することを特徴とする暗号鍵ブロックを用いた情報処理システムにある。

【００１５】さらに、本発明の情報処理システムにおいて、前記キー発行センター（ＫＤＣ）は、複数のエンティテイ各々の識別子と、エンティテイ各々のケイパビリティ情報と、エンティテイ各々のサブ有効化キーブロック（サブＥＫＢ）情報とを対応付けたケイパビリティ管理テーブルを有し、該ケイパビリティ管理テーブルに基づいて、デバイスに対する配信データの処理可能なエンティテイを選択して、該選択エンティテイ配下のデバイスでのみ復号可能な有効化キーブロック（ＥＫＢ）を生成する構成を有することを特徴とする。

【００１６】さらに、本発明の情報処理システムにおいて、前記キーツリーに対する新規追加エンティテイは、該新規エンティテイ内のサブツリー内のノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成し、前記キー発行センター（ＫＤＣ）に対するサブＥＫＢの登録処理を実行するとともに、自己のエンティテイのケイパビリティ情報の通知処理を実行する構成であることを特徴とする。

【００１７】さらに、本発明の情報処理システムにおいて、前記複数のエンティテイは、１つのエンティテイの最下段の末端ノードを他のエンティテイの頂点ノード（サブルート）として構成した上位エンティテイおよび下位エンティテイの階層化構造を有することを特徴とする。

【００１８】さらに、本発明の情報処理システムにおいて、前記複数のエンティテイの各々は、自己のエンティテイに属するサブツリーを構成するノードまたはリーフに対応するキーの設定、更新処理権限を有する構成であることを特徴とする。

【００１９】さらに、本発明の情報処理システムにおいて、前記複数のエンティテイ中、エンティテイ内の最下段リーフを個々のデバイスに対応するリーフとした最下層のエンティテイに属するデバイスの各々は、自己の属するエンティテイの頂点ノード（サブルート）から自己のデバイスに対応するリーフに至るパス上のノード、リーフに設定されたノードキーおよびリーフキーを格納した構成を有することを特徴とする。

【００２０】さらに、本発明の情報処理システムにおいて、前記複数のエンティテイの各々は、自己のエンティテイの下位に、さらに自己管理エンティテイを追加するため、自己のエンティテイ内の最下段のノードまたはリーフ中の１以上のノードまたはリーフをリザーブノードとして保留して設定した構成を有することを特徴とする。

【００２１】さらに、本発明の情報処理システムにおいて、新規エンティテイを末端ノードに追加する上位エンティテイは、新規エンティテイのサブツリーを設定するノードである上位エンティテイ末端ノードに対応するキーを、前記新規エンティテイの頂点ノード（サブルート）キーとして設定する構成であることを特徴とする。

【００２２】さらに、本発明の情報処理システムにおいて、デバイスのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・デバイスに対応するリーフに至るパス上のノードに設定されたノードキーを更新し、更新ノードキーをリボークデバイス以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位

エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボークデバイスからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、デバイスのリボーク処理を実行する構成を有することを特徴とする。

【００２３】さらに、本発明の情報処理システムにおいて、下位エンティテイのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・エンティテイに対応する末端ノードに至るパス上のノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティテイからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティテイ単位のリボーク処理を実行する構成を有することを特徴とする。

【００２４】さらに、本発明の情報処理システムにおいて、下位エンティテイのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・エンティテイに対応する末端ノードに至るパス上の、該末端ノードを除くノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティテイからルートに至るパス上のリボーク・エンティテイに対応する末端ノードを除くノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティテイ単位のリボーク処理を実行する構成を有することを特徴とする。

【００２５】さらに、本発明の第２の側面は、複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する情報処理システムにおける暗号鍵ブロックを用いた情報処理方法において、前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理するエンティテイにおいて、各エンティテイのサブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成するステップと、前記複数のエンティテイのケイパビリティ情報を保有するキー発行センター（ＫＤＣ）において、前記複数のエンティテイのケイパビリティ情報に基づいて、共通のケイパビリティを持つエンティテイの生成するサブ有効化キーブロック（サブＥＫＢ）を抽出し共通のケイパビリティを持つエンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップと、を有することを特徴とする暗号鍵ブロックを用いた情報処理方法にある。

【００２６】さらに、本発明の情報処理方法において、前記キー発行センター（ＫＤＣ）における有効化キーブロック（ＥＫＢ）生成ステップは、共通のケイパビリティを持つエンティテイを選択するエンティテイ選択ステップと、前記エンティテイ選択ステップにおいて選択されたエンティテイによって構成されるエンティテイ・ツリーを生成するステップと、前記エンティテイ・ツリーを構成するノードキーを更新するノードキー更新ステップと、前記ノードキー更新ステップにおいて更新したノードキー、および選択エンティテイのサブＥＫＢに基づいて選択エンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップとを含むことを特徴とする。

【００２７】さらに、本発明の情報処理方法において、前記キー発行センター（ＫＤＣ）は、複数のエンティテイ各々の識別子と、エンティテイ各々のケイパビリティ情報と、エンティテイ各々のサブ有効化キーブロック（サブＥＫＢ）情報とを対応付けたケイパビリティ管理テーブルを有し、該ケイパビリティ管理テーブルに基づいて、デバイスに対する配信データの処理可能なエンティテイを選択して、該選択エンティテイ配下のデバイスでのみ復号可能な有効化キーブロック（ＥＫＢ）を生成することを特徴とする。

【００２８】さらに、本発明の情報処理方法において、前記キーツリーに対する新規追加エンティテイは、該新規エンティテイ内のサブツリー内のノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成し、前記キー発行センター（ＫＤＣ）に対するサブＥＫＢの登録処理を実行するとともに、自己のエンティテイのケイパビリティ情報の通知処理を実行することを特徴とする。

【００２９】さらに、本発明の情報処理方法において、前記複数のエンティテイの各々は、自己のエンティテイに属するサブツリーを構成するノードまたはリーフに対応するキーの設定、更新処理を実行することを特徴とする。

【００３０】さらに、本発明の情報処理方法において、前記情報処理方法において、さらに、新規エンティテイを末端ノードに追加する上位エンティテイは、新規エンティテイのサブツリーを設定するノードである上位エンティテイ末端ノードに対応するキーを、前記新規エンティテイの頂点ノード（サブルート）キーとして設定することを特徴とする。

【００３１】さらに、本発明の情報処理方法において、デバイスのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・デバイスに対応するリーフに至るパス上のノードに設定されたノードキーを更新し、更新ノードキーをリボークデバイス以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボークデバイスからルートに至るパス上のノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、デバイスのリボーク処理を実行することを特徴とする。

【００３２】さらに、本発明の情報処理方法において、下位エンティテイのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・エンティテイに対応する末端ノードに至るパス上のノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティテイからルートに至るパス上のリボーク・エンティテイに対応する末端ノードを除くノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティテイ単位のリボーク処理を実行することを特徴とする。

【００３３】さらに、本発明の情報処理方法において、下位エンティテイのリボーク処理を実行するエンティテイは、エンティテイ内の頂点ノード（サブルート）からリボーク・エンティテイに対応する末端ノードに至るパス上の、該末端ノードを除くノードに設定されたノードキーを更新した更新サブＥＫＢを生成して上位エンティテイに送信し、上位エンティテイは更新サブＥＫＢを提供した末端ノードから自己のサブルートに至るパス上のノードキーを更新した更新サブＥＫＢを生成してさらに上位エンティテイに送信し、最上位エンティテイまで、エンティティ単位での更新サブＥＫＢ生成および送信処理を順次実行して、リボーク・エンティテイからルートに至るパス上のリボーク・エンティテイに対応する末端ノードを除くノードキー更新を行ない、キー更新により生成された更新サブＥＫＢの前記キー発行センター（ＫＤＣ）への登録処理を行なうことにより、エンティテイ単位のリボーク処理を実行することを特徴とする。

【００３４】さらに、本発明の第３の側面は、複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーを構成し、該キーツリーを構成するパスを選択して選択パス上のキー更新、および下位キーによる上位キーの暗号化処理を実行して特定デバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成してデバイスに提供する情報処理システムにおける有効化キーブロック（ＥＫＢ）生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、前記キーツリーの一部を構成し、デバイスのデータ処理能力としてのケイパビリティに基づいて区分されたサブツリーを管理するエンティテイにおいて、各エンティテイのサブツリーに属するノードまたはリーフに対応して設定されるキーのみに基づくサブ有効化キーブロック（サブＥＫＢ）を生成するステップと、前記複数のエンティテイのケイパビリティ情報を保有するキー発行センター（ＫＤＣ）において、前記複数のエンティテイのケイパビリティ情報に基づいて、共通のケイパビリティを持つエンティテイの生成するサブ有効化キーブロック（サブＥＫＢ）を抽出し共通のケイパビリティを持つエンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成するステップと、を含むことを特徴とするプログラム提供媒体にある。

【００３５】

【作用】本発明の構成においては、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キー更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、例えばコンテンツデータの暗号鍵であるコンテンツキーもしくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キーブロックとともに配信する構成としている。このようにすることにより、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

【００３６】さらに、本発明の構成においては、階層的鍵配信ツリーを、管理下のデバイスのデータ処理能力としてのケイパビリティに基づいて区分したサブツリーとしてのエンティテイで管理する構成としてケイパビリティに基づく鍵配信および管理構成を実現している。

【００３７】なお、本発明の第３の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３８】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３９】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４０】

【発明の実施の形態】［システム概要］図1.に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側１０は、コンテンツ受信側２０の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側２０における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画像データ、音声データの再生、あるいは各種プログラムの実行等を行なう。コンテンツの配信側１０とコンテンツ受信側２０との間のデータ交換は、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体を介して実行される。

【００４１】コンテンツの配信側１０のデータ配信手段としては、インターネット１１、衛星放送１２、電話回線１３、ＤＶＤ、ＣＤ等のメディア１４等があり、一方、コンテンツ受信側２０のデバイスとしては、パーソナルコンピュータ（ＰＣ）２１、ポータブルデバイス（ＰＤ）２２、携帯電話、ＰＤＡ（Personal Digital Assistants）等の携帯機器２３、ＤＶＤ、ＣＤプレーヤ等の記録再生器２４、ゲーム端末等の再生専用器２５等がある。これらコンテンツ受信側２０の各デバイスは、コンテンツ配信側１０から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア３０から取得する。

【００４２】［デバイス構成］図２に、図１に示すコンテンツ受信側２０のデバイスの一例として、記録再生装置１００の構成ブロック図を示す。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ（Read Only Memory）１６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０を有し、これらはバス１１０によって相互に接続されている。

【００４３】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００４４】暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００４５】ＲＯＭ１６０は、記録再生装置によって処理されるプログラムデータを格納する。ＣＰＵ１７０は、ＲＯＭ１６０、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。

【００４６】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ

等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００４７】なお、図２に示す暗号処理手段１５０は、１つのワンチップＬＳＩとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

【００４８】［キー配信構成としてのツリー（木）構造について］次に、図１に示すコンテンツ配信側１０からコンテンツ受信側２０の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成およびデータ配信構成を図３を用いて説明する。

【００４９】図３の最下段に示すナンバ０～１５がコンテンツ受信側２０の個々のデバイスである。すなわち図３に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

【００５０】各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図３に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。図３の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【００５１】図３に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図３のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００５２】また、図３のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図３に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００５３】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【００５４】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【００５５】このツリー構造において、図３から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーＫｃｏｎをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を解いてコンテンツキー：Ｋｃｏｎを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【００５６】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そ

のためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【００５７】更新キーの配布処理ついて説明する。キーの更新は、例えば、図４（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図３に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：KeyRenewal Block）と呼ばれることもある。

【００５８】図４（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図４の例は、図３に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図３から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【００５９】図４（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図４（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイスＫ０００００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイスＫ０００００．Ｋ０００１は、図４（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒを得ることができる。なお、図４（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００６０】図３に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０,Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図４（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００６１】図４（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキー：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）ｃｏｎ）を図４（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【００６２】すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【００６３】［ＥＫＢを使用したコンテンツキーの配布］図５に、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図４（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。すなわちＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００６４】図５に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ０００で暗号化して格納する。

【００６５】［ＥＫＢのフォーマット］図６に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージ

ョン６０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ６０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ６０４はタグ部の位置、署名ポインタ６０５は署名の位置を示すポインタである。

【００６６】データ部６０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【００６７】タグ部６０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図７を用いて説明する。図７では、データとして先に図４（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図７の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図７の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図７（ｃ）に示すデータ列、およびタグ列が構成される。

【００６８】タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図４で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）
００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）
０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）
．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【００６９】図６に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【００７０】［ＥＫＢを使用したコンテンツキーおよびコンテンツの配信］上述の例では、コンテンツキーのみをＥＫＢとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、ＥＫＢによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

【００７１】図８にこのデータ構成を示す。図８（ａ）に示す構成において、Ｅｎｃ（Ｋｃｏｎ，ｃｏｎｔｅｎｔ）８０１は、コンテンツ（Content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータであり、Ｅｎｃ（ＫＥＫ，Ｋｃｏｎ）８０２は、コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ：Key Encryption Key）で暗号化したデータであり、Ｅｎｃ（ＥＫＢ，ＫＥＫ）８０３は、コンテンツキー暗号キーＫＥＫを有効化キーブロック（ＥＫＢ）によって暗号化したデータであることを示す。

【００７２】ここで、コンテンツキー暗号キーＫＥＫは、図３で示すノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（ＫＲ）自体であってもよく、またノードキー（Ｋ０００，Ｋ００…）、あるいはルートキー（ＫＲ）によって暗号化されたキーであってもよい。

【００７３】図８（ｂ）は、複数のコンテンツがメディアに記録され、それぞれが同じＥｎｃ（ＥＫＢ，ＫＥＫ）８０５を利用している場合の構成例を示す、このような構成においては、各データに同じＥｎｃ（ＥＫＢ，ＫＥＫ）を付加することなく、Ｅｎｃ（ＥＫＢ，ＫＥＫ）にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【００７４】図９にコンテンツキー暗号キーＫＥＫを、図３に示すノードキーＫ００を更新した更新ノードキーＫ（ｔ）００として構成した場合の例を示す。この場合、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２に対して図９に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）で暗号化したデータと、（ｃ）コンテンツ（content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータとを配信

することにより、デバイス０，１，２はコンテンツを得ることができる。

【００７５】図９の右側には、デバイス０における復号手順を示してある。デバイス０は、まず、受領した有効化キーブロックから自身の保有するリーフキーＫ０００を用いた復号処理により、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号によりコンテンツキーＫｃｏｎを取得し、さらにコンテンツキーＫｃｏｎによりコンテンツの復号を行なう。これらの処理により、デバイス０はコンテンツを利用可能となる。デバイス１，２においても各々異なる処理手順でＥＫＢを処理することにより、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【００７６】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【００７７】このように、ＥＫＢを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【００７８】なお、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツをＤＶＤ、ＣＤ等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック（ＥＫＢ）の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【００７９】図１０に記録媒体に暗号化コンテンツとともに有効化キーブロック（ＥＫＢ）を格納した構成例を示す。図１０に示す例においては、記録媒体にコンテンツＣ１～Ｃ４が格納され、さらに各格納コンテンツに対応するの有効化キーブロック（ＥＫＢ）を対応付けたデータが格納され、さらにバージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が格納されている。例えばＥＫＢ＿１はコンテンツＣ１を暗号化したコンテンツキーＫｃｏｎ１を生成するのに使用され、例えばＥＫＢ＿２はコンテンツＣ２を暗号化したコンテンツキーＫｃｏｎ２を生成するのに使用される。この例では、バージョンＭの有効化キーブロック（ＥＫＢ＿Ｍ）が記録媒体に格納されており、コンテンツＣ３，Ｃ４は有効化キーブロック（ＥＫＢ＿Ｍ）に対応付けられているので、有効化キーブロック（ＥＫＢ＿Ｍ）の復号によりコンテンツＣ３，Ｃ４のコンテンツキーを取得することができる。ＥＫＢ＿１、ＥＫＢ＿２はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なＥＫＢ＿１，ＥＫＢ＿２を取得することが必要となる。

【００８０】図１１に、複数のデバイス間でコンテンツキーが流通する場合のＥＫＢを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。上段（ａ）従来構成であり、下段（ｂ）が本発明の有効化キーブロック（ＥＫＢ）を利用した例である。なお、図１１においてＫａ（Ｋｂ）は、ＫｂをＫａで暗号化したデータであることを示す。

【００８１】（ａ）に示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーＫｓｅｓを共有するために各デバイス間において、認証処理および鍵交換処理（ＡＫＥ：Authentication and Key Exchange）を実行し、認証が成立したことを条件としてセッションキーＫｓｅｓでコンテンツキーＫｃｏｎを暗号化して送信する処理を行なっていた。

【００８２】例えば図１１（ａ）のＰＣにおいては、受信したセッションキーで暗号化したコンテンツキーＫｓｅｓ（Ｋｃｏｎ）をセッションキーで復号してＫｃｏｎを得ることが可能であり、さらに取得したＫｃｏｎをＰＣ自体の保有する保存キーＫｓｔｒで暗号化して自身のメモリに保存することが可能となる。

【００８３】図１１（ａ）において、コンテンツプロバイダは、図１１（ａ）の記録デバイス１１０１にのみデータを利用可能な形で配信したい場合でも、間にＰＣ、再生装置が存在する場合は、図１１（ａ）に示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要となる。また、間に介在するＰＣ、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

【００８４】一方、図１１（ｂ）の下段に示す有効化キーブロック（ＥＫＢ）を利用した例においては、コンテンツプロバイダから有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）の処理によって得られるノードキー、またはルートキーによってコンテンツキーＫｃｏｎを暗号化したデータ（図の例ではＫｒｏｏｔ

（Ｋｃｏｎ））を配信することにより、配信したＥＫＢの処理が可能な機器においてのみコンテンツキーＫｃｏｎを復号して取得することが可能になる。

【００８５】従って、例えば図１１（ｂ）の右端にのみ利用可能な有効化キーブロック（ＥＫＢ）を生成して、その有効化キーブロック（ＥＫＢ）と、そのＥＫＢ処理によって得られるノードキー、またはルートキーによってコンテンツキーＫｃｏｎを暗号化したデータを併せて送ることにより、間に存在するＰＣ、再生機器等は、自身の有するリーフキー、ノードキーによっては、ＥＫＢの処理を実行することができない。従って、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーＫｃｏｎの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

【００８６】ＰＣ、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キーブロック（ＥＫＢ）を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

【００８７】［有効化キーブロック（ＥＫＢ）を使用した認証キーの配信（共通鍵方式）］上述の有効化キーブロック（ＥＫＢ）を使用したデータあるいはキーの配信において、デバイス間で転送される有効化キーブロック（ＥＫＢ）およびコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝走路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理および鍵交換処理を実行することが有効な手段である。ここでは、この認証処理および鍵交換処理を実行する際に使用する認証キーＫａｋｅを上述の有効化キーブロック（ＥＫＢ）を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわちＥＫＢによる暗号化メッセージデータを認証キーとした例である。

【００８８】図１２に、共通鍵暗号方式を用いた相互認証方法（ISO/IEC 9798-2）を示す。図１２においては、共通鍵暗号方式としてＤＥＳを用いているが、共通鍵暗号方式であれば他の方式も可能である。図１２において、まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。なお、鍵Ｋａｂは、ＡおよびＢに共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。ＤＥＳのＣＢＣモードを用いた鍵Ｋａｂによる暗号化処理は、例えばＤＥＳを用いた処理においては、初期値とＲａとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ１を生成し、続けて暗号文Ｅ１とＲｂとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ２を生成し、さらに、暗号文Ｅ２とＩＤ（ｂ）とを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化して生成した暗号文Ｅ３とによって送信データ（Token-AB）を生成する。

【００８９】これを受信したＢは、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵Ｋａｂ（認証キー）で復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を認証キーＫａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を認証キーＫａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を認証キーＫａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)のうち、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【００９０】次にＢは、認証後に使用するセッションキー（Ｋｓｅｓ）を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで認証キーＫａｂを用いて暗号化し、Ａに返送する。

【００９１】これを受信したＡは、受信データを認証キーＫａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッションキーＫｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【００９２】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【００９３】上述の認証処理においては、Ａ，Ｂは共通の認証キーＫａｂを共有する。この共通鍵Ｋａｂを上述の有効化キーブロック（ＥＫＢ）を使用してデバイスに配信する。

【００９４】例えば、図１２の例では、Ａ，またはＢのいずれかが他方が復号可能な有効化キーブロック（ＥＫＢ）を生成して生成した有効化キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して、他方に送信する構成としてもよいし、あるいは第３者がデバイスＡ，Ｂに対して双方が利用可能な有効化キーブロック（ＥＫＢ）を生成してデバイスＡ，Ｂに対して生成した有効化

キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して配信する構成としてもよい。

【００９５】図１３および図１４に複数のデバイスに共通の認証キーＫａｋｅを有効化キーブロック（ＥＫＢ）によって配信する構成例を示す。図１３はデバイス０，１，２，３に対して復号可能な認証キーＫａｋｅを配信する例、図１４はデバイス０，１，２，３中のデバイス３をリボーク（排除）してデバイス０，１，２に対してのみ復号可能な認証キーを配信する例を示す。

【００９６】図１３の例では、更新ノードキーＫ（ｔ）００によって、認証キーＫａｋｅを暗号化したデータ（ｂ）とともに、デバイス０，１，２，３においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーＫ（ｔ）００を復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。それぞれのデバイスは、図１３の右側に示すようにまず、ＥＫＢを処理（復号）することにより、更新されたノードキーＫ（ｔ）００を取得し、次に、取得したノードキーＫ（ｔ）００を用いて暗号化された認証キー：Ｅｎｃ（Ｋ（ｔ）００，Ｋａｋｅ）を復号して認証キーＫａｋｅを得ることが可能となる。

【００９７】その他のデバイス４，５，６，７…は同一の有効化キーブロック（ＥＫＢ）を受信しても自身の保有するノードキー、リーフキーでは、ＥＫＢを処理して更新されたノードキーＫ（ｔ）００を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【００９８】一方、図１４の例は、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２，に対してのみ復号可能な有効化キーブロック（ＥＫＢ）を生成して配信した例である。図１４に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）認証キー（Ｋａｋｅ）をノードキー（Ｋ（ｔ）００）で暗号化したデータを配信する。

【００９９】図１４の右側には、復号手順を示してある。デバイス０，１，２は、まず、受領した有効化キーブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号により認証キーＫａｋｅを取得する。

【０１００】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【０１０１】このように、ＥＫＢを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

【０１０２】［公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信］次に、公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１５を用いて説明する。図１５において、公開鍵暗号方式としてＥＣＣを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１５において、まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび素数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（Ｘ座標とＹ座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。

【０１０３】Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。

【０１０４】次に、Ｂは、素数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１０５】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１０６】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッションキーとして以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成しても

よいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

【０１０７】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１０８】図１６に公開鍵認証と有効化キーブロック（ＥＫＢ）を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとＰＣ間において図１５で説明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なＥＫＢを生成して、更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）とをＰＣ間の認証処理において生成したセッションキーＫｓｅｓで暗号化してＰＣに送信する。

【０１０９】ＰＣはセッションキーで暗号化された［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］をセッションキーで復号した後、再生装置、記録媒体に送信する。

【０１１０】再生装置、記録媒体は、自身の保有するノードキーまたはリーフキーによって［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］を復号することによってコンテンツキーＫｃｏｎを取得する。

【０１１１】この構成によれば、コンテンツプロバイダとＰＣ間での認証を条件として［更新ノードキーによる暗号化を実行したコンテンツキーＥ（Ｋｃｏｎ）と、有効化キーブロック（ＥＫＢ）］が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

【０１１２】［プログラムコードの有効化キーブロック（ＥＫＢ）を使用した配信］上述した例では、コンテンツキー、認証キー等を有効化キーブロック（ＥＫＢ）を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キーブロック（ＥＫＢ）を用いて配信する構成も可能である。すなわちＥＫＢによる暗号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

【０１１３】図１７にプログラムコードを有効化キーブロック（ＥＫＢ）の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス１７０１は、デバイス１７０２の有するノードキー、リーフキーによって復号可能な有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス１７０２に送信する。デバイス１７０２は受信したＥＫＢを処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコードを得る。

【０１１４】図１７に示す例では、さらに、デバイス１７０２において取得したプログラムコードによる処理を実行して、その結果をデバイス１７０１に返して、デバイス１７０１がその結果に基づいて、さらに処理を続行する例を示している。

【０１１５】このように有効化キーブロック（ＥＫＢ）と、有効化キーブロック（ＥＫＢ）に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図３で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

【０１１６】［送信コンテンツに対するチェック値（ＩＣＶ：Integrity Check Value）を対応させる構成］次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値（ＩＣＶ）を生成して、コンテンツに対応付けて、ＩＣＶの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

【０１１７】コンテンツのインテグリティ・チェック値（ＩＣＶ）は、例えばコンテンツに対するハッシュ関数を用いて計算され、ＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２，…）によって計算される。ＫｉｃｖはＩＣＶ生成キーである。Ｃ１，Ｃ２はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号（ＭＡＣ：Message authentication Code）が使用される。

【０１１８】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図１８に示す。図１８の構成に示すように対象となるメッセージを８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。

【０１１９】このようなコンテンツのＭＡＣ値とＩＣＶ生成キーにハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値（ＩＣＶ）が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成したＩＣＶと、新たにコンテンツに基づいて生成したＩＣＶとを比較して同一のＩＣＶが得られればコンテンツに改竄のないことが保証され、ＩＣＶが異なれば、改竄があったと判定される。

【０１２０】［チェック値（ＩＣＶ）の生成キーＫｉｃ

ｖをＥＫＢによって配布する構成］次に、コンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーであるＫｉｃｖを上述の有効化キーブロックによって送付する構成について説明する。すなわちＥＫＢによる暗号化メッセージデータをコンテンツのインテグリティ・チェック値（ＩＣＶ）生成キーとした例である。

【０１２１】図１９および図２０に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キーＫｉｃｖを有効化キーブロック（ＥＫＢ）によって配信する構成例を示す。図１９はデバイス０，１，２，３に対して復号可能なチェック値生成キーＫｉｃｖを配信する例、図２０はデバイス０，１，２，３中のデバイス３をリボーク（排除）してデバイス０，１，２に対してのみ復号可能なチェック値生成キーＫｉｃｖを配信する例を示す。

【０１２２】図１９の例では、更新ノードキーＫ（ｔ）００によって、チェック値生成キーＫｉｃｖを暗号化したデータ（ｂ）とともに、デバイス０，１，２，３においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーＫ（ｔ）００を復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。それぞれのデバイスは、図１９の右側に示すようにまず、ＥＫＢを処理（復号）することにより、更新されたノードキーＫ（ｔ）００を取得し、次に、取得したノードキーＫ（ｔ）００を用いて暗号化されたチェック値生成キー：Ｅｎｃ（Ｋ（ｔ）００，Ｋｉｃｖ）を復号してチェック値生成キーＫｉｃｖを得ることが可能となる。

【０１２３】その他のデバイス４，５，６，７…は同一の有効化キーブロック（ＥＫＢ）を受信しても自身の保有するノードキー、リーフキーでは、ＥＫＢを処理して更新されたノードキーＫ（ｔ）００を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【０１２４】一方、図２０の例は、図３の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２，に対してのみ復号可能な有効化キーブロック（ＥＫＢ）を生成して配信した例である。図２０に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）チェック値生成キー（Ｋｉｃｖ）をノードキー（Ｋ（ｔ）００）で暗号化したデータを配信する。

【０１２５】図２０の右側には、復号手順を示してある。デバイス０，１，２は、まず、受領した有効化キーブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号によりチェック値生成キーＫｉｃｖを取得する。

【０１２６】図３に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【０１２７】このように、ＥＫＢを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【０１２８】このようなコンテンツのインテグリティ・チェック値（ＩＣＶ）を用いることにより、ＥＫＢと暗号化コンテンツの不正コピーを排除することができる。例えば図２１に示すように、コンテンツＣ１とコンテンツＣ２とをそれぞれのコンテンツキーを取得可能な有効化キーブロック（ＥＫＢ）とともに格納したメディア１があり、これをそのままメディア２にコピーした場合を想定する。ＥＫＢと暗号化コンテンツのコピーは可能であり、これをＥＫＢを復号可能なデバイスでは利用できることになる。

【０１２９】図２１の（ｂ）に示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値（ＩＣＶ（Ｃ１，Ｃ２））を格納する構成とする。なお、（ＩＣＶ（Ｃ１，Ｃ２））は、コンテンツＣ１とコンテンツＣ２にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値であるＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２）を示している。図２１の（ｂ）の構成において、メディア１には正当にコンテンツ１とコンテンツ２が格納され、コンテンツＣ１とコンテンツＣ２に基づいて生成されたインテグリティ・チェック値（ＩＣＶ（Ｃ１，Ｃ２））が格納される。また、メディア２には正当にコンテンツ１が格納され、コンテンツＣ１に基づいて生成されたインテグリティ・チェック値（ＩＣＶ（Ｃ１））が格納される。この構成において、メディア１に格納された｛ＥＫＢ，コンテンツ２｝をメディア２にコピーしたとすると、メディア２で、コンテンツチェック値を新たに生成するとＩＣＶ（Ｃ１，Ｃ２）が生成されることになり、メディアに格納されているＫｉｃｖ（Ｃ１）と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにＩＣＶチェックを実行して、生成ＩＣＶと格納ＩＣＶの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

【０１３０】また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値（ＩＣＶ）を書き

換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわちＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，ｃｏｕｎｔｅｒ＋１，Ｃ１，Ｃ２，…）によって計算する構成とする。ここで、カウンタ（ｃｏｕｎｔｅｒ＋１）は、ＩＣＶの書き換えごとに１つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【０１３１】さらに、コンテンツのインテグリティ・チェック値（ＩＣＶ）をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値（ＩＣＶ）をコンテンツとは別のメディア上に格納する構成としてもよい。

【０１３２】例えば、読み込み専用メディアや通常のＭＯ等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値（ＩＣＶ）を格納するとＩＣＶの書き換えが不正なユーザによりなされる可能性があり、ＩＣＶの安全性が保てないおそれがある。この様な場合、ホストマシン上の安全なメディアにＩＣＶを格納して、コンテンツのコピーコントロール（例えばcheck-in/check-out、move）にＩＣＶを使用する構成とすることにより、ＩＣＶの安全な管理およびコンテンツの改竄チェックが可能となる。

【０１３３】この構成例を図２２に示す。図２２では読み込み専用メディアや通常のＭＯ等のコピー防止策のとられていないメディア２２０１にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値（ＩＣＶ）を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア２２０２に格納し、ユーザによる不正なインテグリティ・チェック値（ＩＣＶ）の書き換えを防止した例である。このような構成として、例えばメディア２２０１を装着したデバイスがメディア２２０１の再生を実行する際にホストマシンであるＰＣ、サーバにおいてＩＣＶのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

【０１３４】［階層ツリー構造のカテゴリー分類］暗号鍵をルートキー、ノードキー、リーフキー等、図３の階層ツリー構造として構成し、コンテンツキー、認証キー、ＩＣＶ生成キー、あるいはプログラムコード、データ等を有効化キーブロック（ＥＫＢ）とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリー毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【０１３５】図２３に階層ツリー構造のカテゴリーの分類の一例を示す。図２３において、階層ツリー構造の最上段には、ルートキーＫｒｏｏｔ２３０１が設定され、以下の中間段にはノードキー２３０２が設定され、最下段には、リーフキー２３０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【０１３６】ここで、一例として最上段から第Ｍ段目のあるノードをカテゴリノード２３０４として設定する。すなわち第Ｍ段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第Ｍ段の１つのノードを頂点として以下、Ｍ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【０１３７】例えば図２３の第Ｍ段目の１つのノード２３０５にはカテゴリ［メモリステッイク（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード２３０５以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【０１３８】さらに、Ｍ段から数段分下位の段をサブカテゴリノード２３０６として設定することができる。例えば図に示すようにカテゴリ［メモリスティック］ノード２３０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード２３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード２３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード２３０８と［携帯電話］ノード２３０９を設定することができる。

【０１３９】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【０１４０】このように、１つのノードを頂点としして、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する

構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【０１４１】［簡略ＥＫＢによるキー配信構成］先に説明した例えば図３のツリー構成において、キー、例えばコンテンツキーを所定デバイス（リーフ）宛に送付する場合、キー配布先デバイスの所有しているリーフキー、ノードキーを用いて復号可能な有効化キーブロック（ＥＫＢ）を生成して提供する。例えば図２４（ａ）に示すツリー構成において、リーフを構成するデバイスａ，ｇ，ｊに対してキー、例えばコンテンツキーを送信する場合、ａ，ｇ，ｊの各ノードにおいて復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。

【０１４２】例えば更新ルートキーＫ（ｔ）ｒｏｏｔでコンテンツキーＫ（ｔ）ｃｏｎを暗号化処理し、ＥＫＢとともに配信する場合を考える。この場合、デバイスａ，ｇ，ｊは、それぞれが図２４（ｂ）に示すリーフおよびノードキーを用いて、ＥＫＢの処理を実行してＫ（ｔ）ｒｏｏｔを取得し、取得した更新ルートキーＫ（ｔ）ｒｏｏｔによってコンテンツキーＫ（ｔ）ｃｏｎの復号処理を実行してコンテンツキーを得る。

【０１４３】この場合に提供される有効化キーブロック（ＥＫＢ）の構成は、図２５に示すようになる。図２５に示す有効化キーブロック（ＥＫＢ）は、先の図６で説明した有効化キーブロック（ＥＫＢ）のフォーマットにしたがって構成されたものであり、データ（暗号化キー）と対応するタグとを持つ。タグは、先に図７を用いて説明したように左（Ｌ）、右（Ｒ）、それぞれの方向にデータがあれば０、無ければ１を示している。

【０１４４】有効化キーブロック（ＥＫＢ）を受領したデバイスは、有効化キーブロック（ＥＫＢ）の暗号化キーとタグに基づいて、順次暗号化キーの復号処理を実行して上位ノードの更新キーを取得していく。図２５に示すように、有効化キーブロック（ＥＫＢ）は、ルートからリーフまでの段数（デプス）が多いほど、そのデータ量は増加していく。段数（デプス）は、デバイス（リーフ）数に応じて増大するものであり、キーの配信先となるデバイス数が多い場合は、ＥＫＢのデータ量がさらに増大することになる。

【０１４５】このような有効化キーブロック（ＥＫＢ）のデータ量の削減を可能とした構成について説明する。図２６は、有効化キーブロック（ＥＫＢ）をキー配信デバイスに応じて簡略化して構成した例を示すものである。

【０１４６】図２５と同様、リーフを構成するデバイスａ，ｇ，ｊに対してキー、例えばコンテンツキーを送信する場合を想定する。図２６の（ａ）に示すように、キー配信デバイスによってのみ構成されるツリーを構築する。この場合、図２４（ｂ）に示す構成に基づいて新たなツリー構成として図２６（ｂ）のツリー構成が構築される。ＫｒｏｏｔからＫｊまでは全く分岐がなく１つの枝のみが存在すればよく、ＫｒｏｏｔからＫａおよびＫｇに至るためには、Ｋ０に分岐点を構成するのみで、２分岐構成の図２６（ａ）のツリーが構築される。

【０１４７】図２６（ａ）に示すように、ノードとしてＫ０のみを持つ簡略化したツリーが生成される。更新キー配信のための有効化キーブロック（ＥＫＢ）は、これらの簡略ツリーに基づいて生成する。図２６（ａ）に示すツリーは、有効化キーブロック（ＥＫＢ）を復号可能な末端ノードまたはリーフを最下段とした２分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーである。更新キー配信のための有効化キーブロック（ＥＫＢ）は、この再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成される。

【０１４８】先の図２５で説明した有効化キーブロック（ＥＫＢ）は、各リーフａ，ｇ，ｊからＫｒｏｏｔに至るまでのすべてのキーを暗号化したデータを格納していたが、簡略化ＥＫＢは、簡略化したツリーを構成するノードについてのみの暗号化データを格納する。図２６（ｂ）に示すようにタグは３ビット構成を有する。第１および第２ビットは、図２５の例と、同様の意味を持ち、左（Ｌ）、右（Ｒ）、それぞれの方向にデータがあれば０、無ければ１を示す。第３番目のビットは、ＥＫＢ内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は１、データが無い場合は、０として設定される。

【０１４９】データ通信網、あるいは記憶媒体に格納されてデバイス（リーフ）に提供される有効化キーブロック（ＥＫＢ）は、図２６（ｂ）に示すように、図２５に示す構成に比較すると、データ量が大幅に削減されたものとなる。図２６に示す有効化キーブロック（ＥＫＢ）を受領した各デバイスは、タグの第３ビットに１が格納された部分のデータのみを順次復号することにより、所定の暗号化キーの復号を実現することができる。例えばデバイスａは、暗号化データＥｎｃ（Ｋａ，Ｋ（ｔ）０）をリーフキーＫａで復号して、ノードキーＫ（ｔ）０を取得して、ノードキーＫ（ｔ）０によって暗号化データＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）を復号してＫ（ｔ）ｒｏｏｔを取得する。デバイスｊは、暗号化データＥｎｃ（Ｋｊ，Ｋ（ｔ）ｒｏｏｔ）をリーフキーＫｊで復号して、Ｋ（ｔ）ｒｏｏｔを取得する。

【０１５０】このように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフおよびノードのキー

のみを用いて有効化キーブロック（ＥＫＢ）を生成することにより、少ないデータ量の有効化キーブロック（ＥＫＢ）を生成することが可能となり、有効化キーブロック（ＥＫＢ）のデータ配信が効率的に実行可能となる。

【０１５１】なお、簡略化した階層ツリー構成は、後段で説明するエンティティ単位のＥＫＢ管理構成において特に有効に活用可能である。エンティティは、キー配信構成としてのツリー構成を構成するノードあるいはリーフから選択した複数のノードあるいはリーフの集合体ブロックである。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。１つのエンティティには、ある共通のカテゴリに分類されるデバイスが集まっており、例えば複数のエンティティの頂点ノード（サブルート）によって上述したと同様の簡略化したツリーを再構築してＥＫＢを生成することにより、選択されたエンティティに属するデバイスにおいて復号可能な簡略化された有効化キーブロック（ＥＫＢ）の生成、配信が可能となる。エンティティ単位の管理構成については後段で詳細に説明する。

【０１５２】なお、このような有効化キーブロック（ＥＫＢ）は、光ディスク、ＤＶＤ等の情報記録媒体に格納した構成とすることが可能である。例えば、上述の暗号化キーデータによって構成されるデータ部と、暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（ＥＫＢ）にさらに、更新ノードキーによって暗号化したコンテンツ等のメッセージデータとを格納した情報記録媒体を各デバイスに提供する構成が可能である。デバイスは有効化キーブロック（ＥＫＢ）に含まれる暗号化キーデータをタグ部の識別データにしたがって順次抽出して復号し、コンテンツの復号に必要なキーを取得してコンテンツの利用を行なうことが可能となる。もちろん、有効化キーブロック（ＥＫＢ）をインターネット等のネットワークを介して配信する構成としてもよい。

【０１５３】［エンティティ単位のＥＫＢ管理構成］次に、キー配信構成としてのツリー構成を構成するノードあるいはリーフを、複数のノードあるいはリーフの集合としてのブロックで管理する構成について説明する。なお、複数のノードあるいはリーフの集合としてのブロックを以下エンティティと呼ぶ。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。すなわち、エンティティは、デバイス種類、サービス種類、管理手段種類等の共通のカテゴリに属するデバイスあるいはエンティティの管理主体として定義される。

【０１５４】エンティティについて、図２７を用いて説明する。図２７（ａ）はツリーのエンティティ単位での管理構成を説明する図である。１つのエンティティは図では、三角形として示し、例えば１エンティティ２７０１内には、複数のノードが含まれる。１エンティティ内のノード構成を示すのが（ｂ）である。１つのエンティティは、１つのノードを頂点とした複数段の２分岐形ツリーによって構成される。以下、エンティティの頂点ノード２７０２をサブルートと呼ぶ。

【０１５５】ツリーの末端は、（ｃ）に示すようにリーフ、すなわちデバイスによって構成される。デバイスは、複数デバイスをリーフとし、サブルートである頂点ノード２７０２を持つツリーによって構成されるいずれかのエンティティに属する。

【０１５６】図２７（ａ）から理解されるように、エンティティは、階層構造を持つ。この階層構造について、図２８を用いて説明する。

【０１５７】図２８（ａ）は、階層構造を簡略化して説明するための図であり、Ｋｒｏｏｔから数段下の段にエンティティＡ０１～Ａｎｎが構成され、エンティティＡ１～Ａｎの下位には、さらに、エンティティＢ０１～Ｂｎｋ、さらに、その下位にエンティティＣ１～Ｃｎｑが設定されている。各エンティティは、図２８（ｂ），（ｃ）に示す如く、複数段のノード、リーフによって構成されるツリー形状を持つ。

【０１５８】例えばエンティティＢｎｋの構成は、（ｂ）に示すように、サブルート２８１１を頂点ノードとして、末端ノード２８１２に至るまでの複数ノードを有する。このエンティティは識別子Ｂｎｋを持ち、エンティティＢｎｋ内のノードに対応するノードキー管理をエンティティＢｎｋ独自に実行することにより、末端ノード２８１２を頂点として設定される下位（子）エンティティの管理を実行する。また、一方、エンティティＢｎｋは、サブルート２８１１を末端ノードとして持つ上位（親）エンティティＡｎｎの管理下にある。

【０１５９】エンティティＣｎ３の構成は、（ｃ）に示すように、サブルート２８５１を頂点ノードとして、各デバイスである末端ノード２８５２、この場合はリーフに至るまで複数ノード、リーフを有する。このエンティティは識別子Ｃｎ３を持ち、エンティティＣｎ３内のノード、リーフに対応するノードキー、リーフキー管理をエンティティＣｎ３独自に実行することにより、末端ノード２８５２に対応するリーフ（デバイス）の管理を実行する。また、一方、エンティティＣｎ３は、サブルート２８５１を末端ノードとして持つ上位（親）エンティティＢｎ２の管理下にある。各エンティティにおけるキー管理とは、例えばキー更新処理、リボーク処理等であるが、これらは後段で詳細に説明する。

【０１６０】最下段エンティティのリーフであるデバイ

スには、デバイスの属するエンティティのリーフキーから、自己の属するエンティティの頂点ノードであるサブルートノードに至るパスに位置する各ノードのノードキーおよびリーフキーが格納される。例えば末端ノード２８５２のデバイスは、末端ノード（リーフ）２８５２から、サブルートノード２８５１までの各キーを格納する。

【０１６１】図２９を用いて、さらにエンティティの構成について説明する。エンティティは様々な段数によって構成されるツリー構造を持つことが可能である。段数、すなわちデプス（depth）は、エンティティで管理する末端ノードに対応する下位（子）エンティティの数、あるいはリーフとしてのデバイス数に応じて設定可能である。

【０１６２】図２９の（ａ）に示すような上下エンティティ構成を具体化すると、（ｂ）に示す態様となる。ルートエンティティは、ルートキーを持つ最上段のエンティティである。ルートエンティティの末端ノードに複数の下位エンティティとしてエンティティＡ，Ｂ，Ｃが設定され、さらに、エンティティＣの下位エンティティとしてエンティティＤが設定される。エンティティＣは２９０１は、その末端ノードの１つ以上のノードをリザーブノード２９５０として保持し、自己の管理するエンティティを増加させる場合、さらに複数段のツリー構成を持つエンティティＣ’２９０２をリザーブノード２９５０を頂点ノードとして新設することにより、管理末端ノード２９７０を増加させて、管理末端ノードに増加した下位エンティティを追加することができる。

【０１６３】リザーブノードについて、さらに図３０を用いて説明する。エンティティＡ，３０１１は、管理する下位エンティティＢ，Ｃ，Ｄ…を持ち、１つのリザーブノード３０２１を持つ。エンティティは管理対象の下位エンティティをさらに増加させたい場合、リザーブノード３０２１に、自己管理の下位エンティティＡ’，３０１２を設定し、下位エンティティＡ’，３０１２の末端ノードにさらに管理対象の下位エンティティＦ，Ｇを設定することができる。自己管理の下位エンティティＡ’，３０１２も、その末端ノードの少なくとも１つをリザーブノード３０２２として設定することにより、さらに下位エンティティＡ’’３０１３を設定して、さらに管理エンティティを増加させることができる。下位エンティティＡ’’３０１３の末端ノードにも１以上のリザーブノードを確保する。このようなリザーブノード保有構成をとることにより、あるエンティティの管理する下位エンティティは、際限なく増加させることが可能となる。なお、リザーブエンティティは、末端ノードの１つのみではなく、複数個設定する構成としてもよい。

【０１６４】それぞれのエンティティでは、エンティティ単位で有効化キーブロック（ＥＫＢ）が構成され、エンティティ単位でのキー更新、リボーク処理を実行することになる。図３０のように複数のエンティティＡ，Ａ’，Ａ’’には各エンティティ個々の有効化キーブロック（ＥＫＢ）が設定されることになるが、これらは、エンティティＡ，Ａ’，Ａ’’を共通に管理する例えばあるデバイスメーカーが一括して管理することが可能である。

【０１６５】［新規エンティティの登録処理］次に、新規エンティティの登録処理について説明する。登録処理シーケンスを図３１に示す。図３１のシーケンスにしたがって説明する。新たにツリー構成中に追加される新規（子）エンティティ（Ｎ－Ｅｎ）は、上位（親）エンティティ（Ｐ－Ｅｎ）に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ（Ｐ－Ｅｎ）に送付する。

【０１６６】登録要求を受領した上位エンティティ（Ｐ－Ｅｎ）は、受領した新規（子）エンティティ（Ｎ－Ｅｎ）の公開鍵を証明書発行局（ＣＡ：Certificate Authority）に転送し、ＣＡの署名を付加した新規（子）エンティティ（Ｎ－Ｅｎ）の公開鍵を受領する。これらの手続きは、上位エンティティ（Ｐ－Ｅｎ）と新規（子）エンティティ（Ｎ－Ｅｎ）との相互認証の手続きとして行われる。

【０１６７】これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ（Ｐ－Ｅｎ）は、新規（子）エンティティ（Ｎ－Ｅｎ）の登録を許可し、新規（子）エンティティ（Ｎ－Ｅｎ）のノードキーを新規（子）エンティティ（Ｎ－Ｅｎ）に送信する。このノードキーは、上位エンティティ（Ｐ－Ｅｎ）の末端ノードの１つのノードキーであり、かつ、新規（子）エンティティ（Ｎ－Ｅｎ）の頂点ノード、すなわちサブルートキーに対応する。

【０１６８】このノードキー送信が終了すると、新規（子）エンティティ（Ｎ－Ｅｎ）は、新規（子）エンティティ（Ｎ－Ｅｎ）のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティティ内の有効化キーブロック（ＥＫＢ）を生成する。１つのエンティティ内の有効化キーブロック（ＥＫＢ）をサブＥＫＢと呼ぶ。

【０１６９】一方、上位エンティティ（Ｐ－Ｅｎ）は、新規（子）エンティティ（Ｎ－Ｅｎ）の追加により、有効化する末端ノードを追加した上位エンティティ（Ｐ－Ｅｎ）内のサブＥＫＢを生成する。

【０１７０】新規（子）エンティティ（Ｎ－Ｅｎ）は、新規（子）エンティティ（Ｎ－Ｅｎ）内のノードキー、リーフキーによって構成されるサブＥＫＢを生成すると、これを上位エンティティ（Ｐ－Ｅｎ）に送信する。

【０１７１】新規（子）エンティティ（Ｎ－Ｅｎ）からサブＥＫＢを受信した上位エンティティ（Ｐ－Ｅｎ）

は、受信したサブＥＫＢと、上位エンティテイ（Ｐ－Ｅｎ）の更新したサブＥＫＢとをキー発行センター（ＫＤＣ：Key Distribute Center）に送信する。

【０１７２】キー発行センター（ＫＤＣ）は、すべてのエンティテイのサブＥＫＢに基づいて、様々な態様のＥＫＢ、すなわち特定のエンティテイあるいはデバイスのみが復号可能なＥＫＢを生成することが可能となる。このように復号可能なエンティテイあるいはデバイスを設定したＥＫＢを例えばコンテンツプロバイダに提供し、コンテンツプロバイダがＥＫＢに基づいてコンテンツキーを暗号化して、ネットワークを介して、あるいは記録媒体に格納して提供することにより、特定のデバイスでのみ利用可能なコンテンツを提供することが可能となる。

【０１７３】なお、新規エンティテイのサブＥＫＢのキー発行センター（ＫＤＣ）に対する登録処理は、サブＥＫＢを上位エンティテイを介してを順次転送して実行する方法に限るものではなく、上位エンティテイを介さずに、新規登録エンティテイから直接、キー発行センター（ＫＤＣ）に登録する処理を実行する構成としてもよい。

【０１７４】上位エンティテイと、上位エンティテイに新規追加する下位エンティテイとの対応について図３２を用いて説明する。上位エンティテイの末端ノードの１つ３２０１を新規追加エンティテイの頂点ノードとして、下位エンティテイに提供することによって下位エンティテイは、上位エンティテイの管理下のエンティテイとして追加される。上位エンティテイの管理下のエンティテイとは、後段で詳細に説明するが、下位エンティテイのリボーク（排除）処理を上位エンティテイが実行できる構成であるという意味を含むものである。

【０１７５】図３２に示すように、上位エンティテイに新規エンティテイが設定されると、上位エンティテイのリーフである末端ノードの１つのノード３２０１と新規追加エンティテイの頂点ノード３２０２とが等しいノードとして設定される。すなわち上位ノードの１つのリーフである１つの末端ノードが、新規追加エンティテイのサブルートとして設定される。このように設定されることにより、新規追加エンティテイが全体ツリー構成の下で有効化される。

【０１７６】図３３に新規追加エンティテイを設定した際に上位エンティテイが生成する更新ＥＫＢの例を示す。図３３は、（ａ）に示す構成、すなわち既に有効に存在する末端ノード（ｎｏｄｅ０００）３３０１と末端ノード（ｎｏｄｅ００１）３３０２があり、ここに新規追加エンティテイに新規エンティテイ追加末端ノード（ｎｏｄｅ１００）３３０３を付与した際に上位エンティテイが生成するサブＥＫＢの例を示したものである。

【０１７７】サブＥＫＢは、図３３の（ｂ）に示すようにな構成を持つ。それぞれ有効に存在する末端ノードキーにより暗号化された上位ノードキー、上位ノードキーで暗号化されたさらなる上位ノードキー、…さらに上位に進行してサブルートキーに至る構成となっている。この構成によりサブＥＫＢが生成される。各エンティテイは図３３（ｂ）に示すと同様、有効な末端ノード、あるいはリーフキーにより暗号化された上位ノードキー、上位ノードキーでさらに上位のノードキーを暗号化し、順次上位に深厚してサブルートに至る暗号化データによって構成されるＥＫＢを有し、これを管理する。

【０１７８】［エンティテイ管理下におけるリボーク処理］次に、キー配信ツリー構成をエンティテイ単位として管理する構成におけるデバイスあるいはエンティテイのリボーク（排除）処理について説明する。先の図３，４では、ツリー構成全体の中から特定のデバイスのみ復号可能で、リボークされたデバイスは復号不可能な有効化キーブロック（ＥＫＢ）を配信する処理について説明した。図３，４で説明したリボーク処理は、ツリー全体の中から特定のリーフであるデバイスをリボークする処理であったが、ツリーのエンティテイ管理による構成では、エンティテイ毎にリボーク処理が実行可能となる。

【０１７９】図３４以下の図を用いてエンティテイ管理下のツリー構成におけるリボーク処理について説明する。図３４は、ツリーを構成するエンティテイのうち、最下段のエンティテイ、すなわち個々のデバイスを管理しているエンティテイによるデバイスのリボーク処理を説明する図である。

【０１８０】図３４（ａ）は、エンティテイ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティテイＡ０１～Ａｎｎ、さらにその下位段にＢ０１～Ｂｎｋのエンティテイ、さらにその下位段にＣ１～ｃｎのエンティテイが構成されている。最も下のエンティテイは、末端ノード（リーフ）が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

【０１８１】ここで、リボーク処理は、各エンティテイにおいて独自に実行される。例えば、最下段のエンティテイＣ１～Ｃｎでは、リーフのデバイスのリボーク処理が実行される。図３４（ｂ）には、最下段のエンティテイの１つであるエンティテイＣｎ，３４３０のツリー構成を示している。エンティテイＣｎ，３４３０は、頂点ノード３４３１を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

【０１８２】この末端ノードであるリーフ中に、リボーク対象となるデバイス、例えばデバイス３４３２があったとすると、エンティテイＣｎ，３４３０は、独自に更新したエンティテイＣｎ内のノードキー、リーフキーによって構成される有効化キーブロック（サブＥＫＢ）を生成する。この有効化キーブロックは、リボークデバイス３４３２においては復号できず、他のリーフを構成するデバイスにおいてのみ復号可能な暗号化キーにより構

成されるキーブロックである。エンティテイＣｎの管理者は、これを更新されたサブＥＫＢとして生成する。具体的には、サブルートからリボークデバイス３４３２に連なるパスを構成する各ノード３４３１，３４３４，３４３５のノードキーを更新して、この更新ノードキーをリボークデバイス３４３２以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成したブロックを更新サブＥＫＢとする。この処理は、先の図３，４において説明したリボーク処理構成において、ルートキーを、エンティテイの頂点キーであるサブルートキーに置き換えた処理に対応する。

【０１８３】このようにエンティテイＣｎ，３４３０がリボーク処理によって更新した有効化キーブロック（サブＥＫＢ）は、上位エンティテイに送信される。この場合、上位エンティテイはエンティテイＢｎｋ，３４２０であり、エンティテイＣｎ，３４３０の頂点ノード３４３１を末端ノードとして有するエンティテイである。

【０１８４】エンティテイＢｎｋ，３４２０は、下位エンティテイＣｎ，３４３０から有効化キーブロック（サブＥＫＢ）を受領すると、そのキーブロックに含まれるエンティテイＣｎｋ，３４３０の頂点ノード３４３１に対応するエンティテイＢｎｋ，３４２０の末端ノード３４３１を、下位エンティテイＣｎ，３４３０において更新されたキーに設定して、自身のエンティテイＢｎｋ，３４２０のサブＥＫＢの更新処理を実行する。図３４（ｃ）にエンティテイＢｎｋ，３４２０のツリー構成を示す。エンティテイＢｎｋ，３４２０において、更新対象となるノードキーは、図３４（ｃ）のサブルート３４２１からリボークデバイスを含むエンティテイを構成する末端ノード３４３１に至るパス上のノードキーである。すなわち、更新サブＥＫＢを送信してきたエンティテイのノード３４３１に連なるパスを構成する各ノード３４２１，３４２４，３４２５のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティテイＢｎｋ，３４２０の新たな更新サブＥＫＢを生成する。

【０１８５】さらに、エンティテイＢｎｋ，３４２０が更新した有効化キーブロック（サブＥＫＢ）は、上位エンティテイに送信される。この場合、上位エンティテイはエンティテイＡｎｎ，３４１０であり、エンティテイＢｎｋ，３４２０の頂点ノード３４２１を末端ノードとして有するエンティテイである。

【０１８６】エンティテイＡｎｎ，３４１０は、下位エンティテイＢｎｋ，３４２０から有効化キーブロック（サブＥＫＢ）を受領すると、そのキーブロックに含まれるエンティテイＢｎｋ，３４２０の頂点ノード３４２１に対応するエンティテイＡｎｎ，３４１０の末端ノード３４２１を、下位エンティテイＢｎｋ，３４２０において更新されたキーに設定して、自身のエンティテイＡｎｎ，３４１０のサブＥＫＢの更新処理を実行する。図３４（ｄ）にエンティテイＡｎｎ，３４１０のツリー構成を示す。エンティテイＡｎｎ，３４１０において、更新対象となるノードキーは、図３４（ｄ）のサブルート３４１１から更新サブＥＫＢを送信してきたエンティテイのノード３４２１に連なるパスを構成する各ノード３４１１，３４１４，３４１５のノードキーである。これら各ノードのノードキーを更新してエンティテイＡｎｎ，３４１０の新たな更新サブＥＫＢを生成する。

【０１８７】これらの処理を順次、上位のエンティテイにおいて実行し、図２９（ｂ）で説明したルートエンティテイまで実行する。この一連の処理により、デバイスのリボーク処理が完結する。なお、それぞれのエンティテイにおいて更新されたサブＥＫＢは、最終的にキー発行センター（ＫＤＣ）に送信され、保管される。キー発行センター（ＫＤＣ）は、すべてのエンティテイの更新サブＥＫＢに基づいて、様々なＥＫＢを生成する。更新ＥＫＢは、リボークされたデバイスでの復号が不可能な暗号化キーブロックとなる。

【０１８８】デバイスのリボーク処理のシーケンス図を図３５に示す。処理手順を図３５のシーケンス図に従って説明する。まず、ツリー構成の最下段にあるデバイス管理エンティテイ（Ｄ－Ｅｎ）は、デバイス管理エンティテイ（Ｄ－Ｅｎ）内のリボーク対象のリーフを排除するために必要なキー更新を行ない、デバイス管理エンティテイ（Ｄ－Ｅｎ）の新たなサブＥＫＢ（Ｄ）を生成する。更新サブＥＫＢ（Ｄ）は、上位エンティテイに送付される。更新サブＥＫＢ（Ｄ）を受領した上位（親）エンティテイ（Ｐ１－Ｅｎ）は、更新サブＥＫＢ（Ｄ）の更新頂点ノードに対応した末端ノードキーの更新および、その末端ノードからサブルートに至るパス上のノードキーを更新した更新サブＥＫＢ（Ｐ１）を生成する。これらの処理を順次、上位エンティテイにおいて実行して、最終的に更新されたすべてのサブＥＫＢがキー発行センター（ＫＤＣ）に格納され管理される。

【０１８９】図３６にデバイスのリボーク処理によって上位エンティテイが更新処理を行なって生成する有効化キーブロック（ＥＫＢ）の例を示す。

【０１９０】図３６は、（ａ）に示す構成において、リボークデバイスを含む下位エンティテイから更新サブＥＫＢを受信した上位エンティテイにおいて生成するＥＫＢの例を説明する図である。リボークデバイスを含む下位エンティテイの頂点ノードは、上位エンティテイの末端ノード（ｎｏｄｅ１００）３６０１に対応する。

【０１９１】上位エンティテイは、上位エンティテイのサブルートから末端ノード（ｎｏｄｅ１００）３６０１までのパスに存在するノードキーを更新して新たな更新サブＥＫＢを生成する。更新サブＥＫＢは、図３６（ｂ）のようになる。更新されたキーは、下線および［’］を付して示してある。このように更新された末端ノードからサブルートまでのパス上のノードキーを更

新してそのエンティティにおける更新サブＥＫＢとする。

【０１９２】次に、リボークする対象をエンティティとした場合の処理、すなわちエンティティのリボーク処理について説明する。

【０１９３】図３７（ａ）は、エンティティ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティティＡ０１～Ａｎｎ、さらにその下位段にＢ０１～Ｂｎｋのエンティティ、さらにその下位段にＣ１～ｃｎのエンティティが構成されている。最も下のエンティティは、末端ノード（リーフ）が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

【０１９４】ここで、リボーク処理を、エンティティＣｎ，３７３０に対して実行する場合について説明する。最下段のエンティティＣｎ，３７３０は、図３７（ｂ）に示すように頂点ノード３４３１を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

【０１９５】エンティティＣｎ，３７３０をリボークすることにより、エンティティＣｎ，３７３０に属するすべてのデバイスのツリー構造からの一括排除が可能となる。エンティティＣｎ，３７３０のリボーク処理は、エンティティＣｎ，３７３０の上位エンティティであるエンティティＢｎｋ，３７２０において実行される。エンティティＢｎｋ，３７２０は、エンティティＣｎ，３７３０の頂点ノード３７３１を末端ノードとして有するエンティティである。

【０１９６】エンティティＢｎｋ，３７２０は、下位エンティティＣｎ，３７３０のリボークを実行する場合、エンティティＣｎｋ，３７３０の頂点ノード３７３１に対応するエンティティＢｎｋ，３７２０の末端ノード３７３１を更新し、さらに、そのリボークエンティティ３７３０からエンティティＢｎｋ，３７２０のサブルートまでのパス上のノードキーの更新を行ない有効化キーブロックを生成して更新サブＥＫＢを生成する。更新対象となるノードキーは、図３７（ｃ）のサブルート３７２１からリボークエンティティの頂点ノードを構成する末端ノード３７３１に至るパス上のノードキーである。すなわち、ノード３７２１，３７２４，３７２５，３７３１のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティティＢｎｋ，３７２０の新たな更新サブＥＫＢを生成する。

【０１９７】あるいは、エンティティＢｎｋ，３７２０は、下位エンティティＣｎ，３７３０のリボークを実行する場合、エンティティＣｎｋ，３７３０の頂点ノード３７３１に対応するエンティティＢｎｋ，３７２０の末端ノード３７３１は更新せず、そのリボークエンティティ３７３０からエンティティＢｎｋ，３７２０のサブルートまでのパス上の末端ノード３７３１を除くノードキーの更新を行ない有効化キーブロックを生成して更新サブＥＫＢを生成してもよい。

【０１９８】さらに、エンティティＢｎｋ，３７２０が更新した有効化キーブロック（サブＥＫＢ）は、上位エンティティに送信される。この場合、上位エンティティはエンティティＡｎｎ，３７１０であり、エンティティＢｎｋ，３７２０の頂点ノード３７２１を末端ノードとして有するエンティティである。

【０１９９】エンティティＡｎｎ，３７１０は、下位エンティティＢｎｋ，３７２０から有効化キーブロック（サブＥＫＢ）を受領すると、そのキーブロックに含まれるエンティティＢｎｋ，３７２０の頂点ノード３７２１に対応するエンティティＡｎｎ，３７１０の末端ノード３７２１を、下位エンティティＢｎｋ，３７２０において更新されたキーに設定して、自身のエンティティＡｎｎ，３７１０のサブＥＫＢの更新処理を実行する。図３７（ｄ）にエンティティＡｎｎ，３７１０のツリー構成を示す。エンティティＡｎｎ，３７１０において、更新対象となるノードキーは、図３７（ｄ）のサブルート３７１１から更新サブＥＫＢを送信してきたエンティティのノード３７２１に連なるパスを構成する各ノード３７１１，３７１４，３７１５のノードキーである。これら各ノードのノードキーを更新してエンティティＡｎｎ，３７１０の新たな更新サブＥＫＢを生成する。

【０２００】これらの処理を順次、上位のエンティティにおいて実行し、図２９（ｂ）で説明したルートエンティティまで実行する。この一連の処理により、エンティティのリボーク処理が完結する。なお、それぞれのエンティティにおいて更新されたサブＥＫＢは、最終的にキー発行センター（ＫＤＣ）に送信され、保管される。キー発行センター（ＫＤＣ）は、すべてのエンティティの更新サブＥＫＢに基づいて、様々なＥＫＢを生成する。更新ＥＫＢは、リボークされたエンティティに属するデバイスでの復号が不可能な暗号化キーブロックとなる。

【０２０１】エンティティのリボーク処理のシーケンス図を図３８に示す。処理手順を図３８のシーケンス図に従って説明する。まず、エンティティをリボークしようとするエンティティ管理エンティティ（Ｅ－Ｅｎ）は、エンティティ管理エンティティ（Ｅ－Ｅｎ）内のリボーク対象の末端ノードを排除するために必要なキー更新を行ない、エンティティ管理エンティティ（Ｅ－Ｅｎ）の新たなサブＥＫＢ（Ｅ）を生成する。更新サブＥＫＢ（Ｅ）は、上位エンティティに送付される。更新サブＥＫＢ（Ｅ）を受領した上位（親）エンティティ（Ｐ１－Ｅｎ）は、更新サブＥＫＢ（Ｅ）の更新頂点ノードに対応した末端ノードキーの更新および、その末端ノードからサブルートに至るパス上のノードキーを更新した更新サブＥＫＢ（Ｐ１）を生成する。これらの処理を順次、上位エンティティにおいて実行して、最終的に更新されたすべてのサブＥＫＢがキー発行センター（ＫＤＣ）に格納され管理される。キー発行センター（ＫＤＣ）は、

すべてのエンティテイの更新サブＥＫＢに基づいて、様々なＥＫＢを生成する。更新ＥＫＢは、リボークされたエンティテイに属するデバイスでの復号が不可能な暗号化キーブロックとなる。

【０２０２】図３９にリボークされた下位エンティテイと、リボークを行なった上位エンティテイの対応を説明する図を示す。上位エンティテイの末端ノード３９０１は、エンティテイのリボークにより更新され、上位エンティテイのツリーにおける末端ノード３９０１からサブルートまでのパスに存在するノードキーの更新により、新たなサブＥＫＢが生成される。その結果、リボークされた下位エンティテイの頂点ノード３９０２のノードキーと、上位エンティテイの末端ノード３９０１のノードキーは不一致となる。エンティテイのリボーク後にキー発行センター（ＫＤＣ）によって生成されるＥＫＢは、上位エンティテイにおいて更新された末端ノード３９０１のキーに基づいて生成されることになるので、その更新キーを保有しない下位エンティテイのリーフに対応するデバイスは、キー発行センター（ＫＤＣ）によって生成されるＥＫＢの復号ガ不可能になる。

【０２０３】なお、上述の説明では、デバイスを管理する最下段のエンティテイのリボーク処理について説明したが、ツリーの中段にあるエンティテイ管理エンティテイをその上位エンティテイがリボークする処理も上記と同様のプロセスによって可能である。中段のエンティティ管理エンティテイをリボークすることにより、リボークされたエンティテイ管理エンティテイの下位に属するすべての複数エンティテイおよびデバイスを一括してリボーク可能となる。

【０２０４】このように、エンティテイ単位でのリボークを実行することにより、１つ１つのデバイス単位で実行するリボーク処理に比較して簡易なプロセスでのリボーク処理が可能となる。

【０２０５】［エンティテイのケイパビリティ管理］次に、エンティテイ単位でのキー配信ツリー構成において、各エンティティの許容するケイパビリティ(Capability)を管理して、ケイパビリティに応じたコンテンツ配信を行なう処理構成について説明する。ここでケイパビリティとは、例えば特定の圧縮音声データの復号が可能であるとか、特定の音声再生方式を許容するとか、あるいは特定の画像処理プログラムを処理できる等、デバイスがどのようなコンテンツ、あるいはプログラム等を処理できるデバイスであるか、すなわちデバイスのデータ処理能力の定義情報である。

【０２０６】図４０にケイパビリティを定義したエンティテイ構成例を示す。キー配信ツリー構成の最頂点にルートノードが位置し、下層に複数のエンティテイが接続されて各ノードが２分岐を持つツリー構成である。ここで、例えばエンティテイ４００１は、音声再生方式Ａ，Ｂ，Ｃのいずれかを許容するケイパビリティを持つエンティテイとして定義される。具体的には、例えばある音声圧縮プログラムーＡ、Ｂ、またはＣ方式で圧縮した音楽データを配信した場合に、エンティテイ４００１以下に構成されたエンティテイに属するデバイスは圧縮データを伸長する処理が可能である。

【０２０７】同様にエンティテイ４００２は音声再生方式ＢまたはＣ、エンティテイ４００３は音声再生方式ＡまたはＢ、エンティテイ４００４は音声再生方式Ｂ、エンティテイ４００５は音声再生方式Ｃを処理することが可能なケイパビリティを持つエンティテイとして定義される。

【０２０８】一方、エンティテイ４０２１は、画像再生方式ｐ，ｑ，ｒを許容するエンティテイとして定義され、エンティテイ４０２２は方式ｐ，ｑの画像再生方式、エンティテイ４０２３は方式ｐの画像再生が可能なケイパビリティを持つエンティテイとして定義される。

【０２０９】このような各エンティテイのケイパビリティ情報は、キー発行センター（ＫＤＣ）において管理される。キー発行センター（ＫＤＣ）は、例えばあるコンテンツプロバイダが特定の圧縮プログラムで圧縮した音楽データを様々なデバイスに配信したい場合、その特定の圧縮プログラムを再生可能なデバイスに対してのみ復号可能な有効化キーブロック（ＥＫＢ）を各エンティテイのケイパビリティ情報に基づいて生成することができる。コンテンツを提供するコンテンツプロバイダは、ケイパビリティ情報に基づいて生成した有効化キーブロック（ＥＫＢ）によって暗号化したコンテンツキーを配信し、そのコンテンツキーで暗号化した圧縮音声データを各デバイスに提供する。この構成により、データの処理が可能なデバイスに対してのみ特定の処理プログラムを確実に提供することが可能となる。

【０２１０】なお、図４０では全てのエンティテイについてケイパビリティ情報を定義している構成であるが、図４０の構成ようにすべてのエンティテイにケイパビリティ情報を定義することは必ずしも必要ではなく、例えば図４１に示すようにデバイスが属する最下段のエンティテイについてのみケイパビリティを定義して、最下段のエンティテイに属するデバイスのケイパビリティをキー発行センター（ＫＤＣ）において管理して、コンテンツプロバイダが望む処理の可能なデバイスにのみ復号可能な有効化キーブロック（ＥＫＢ）を最下段のエンティテイに定義されたケイパビリティ情報に基づいて生成する構成としてもよい。図４１では、末端ノードにデバイスが定義されたエンティテイ４１０１＝４１０５におけるケイパビリテイが定義され、これらのエンティテイについてのケイパビリティをキー発行センター（ＫＤＣ）において管理する構成である。例えばエンティテイ４１０１には音声再生については方式Ｂ、画像再生については方式ｒの処理が可能なデバイスが属している。エンティテイ４１０２には音声再生については方式Ａ、画像再

生については方式ｑの処理が可能なデバイスが属している等である。

【０２１１】図４２にキー発行センター（ＫＤＣ）において管理するケイパビリティ管理テーブルの構成例を示す。ケイパビリティ管理テーブルは、図４２（ａ）のようなデータ構成を持つ。すなわち、各エンティティを識別する識別子としてのエンティティＩＤ、そのエンティティに定義されたケイパビリティを示すケイパビリティリスト、このケイパビリティリストは図４２（ｂ）に示すように、例えば音声データ再生処理方式（Ａ）が処理可能であれば［１］、処理不可能であれは［０］、音声データ再生処理方式（Ｂ）が処理可能であれば［１］、処理不可能であれは［０］…等、様々な態様のデータ処理についての可否を１ビットづつ［１］または［０］を設定して構成されている。なお、このケイパビリティ情報の設定方法はこのような形式に限らず、エンティティの管理デバイスについてのケイパビリティを識別可能であれば他の構成でもよい。

【０２１２】ケイパビリティ管理テーブルには、さらに、各エンティティのサブＥＫＢ、あるいはサブＥＫＢが別のデータベースに格納されている場合は、サブＥＫＢの識別情報が格納され、さらに、各エンティティのサブルートノード識別データが格納される。

【０２１３】キー発行センター（ＫＤＣ）は、ケイパビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キーブロック（ＥＫＢ）を生成する。図４３を用いて、ケイパビリティ情報に基づく有効化キーブロックの生成処理について説明する。

【０２１４】まず、ステップＳ４３０１において、キー発行センター（ＫＤＣ）は、ケイパビリティ管理テーブルから、指定されたケイパビリティを持つエンティティを選択する。具体的には、例えばコンテンツプロバイダが音声データ再生処理方式Ａに基づく再生可能なデータを配信したい場合は、図４２（ａ）のケイパビリティリストから、例えば音声データ再生処理（方式Ａ）の項目が［１］に設定されたエンティティを選択する。

【０２１５】次に、ステップＳ４３０２において、選択されたエンティティによって構成される選択エンティティＩＤのリストを生成する。次に、ステップＳ４３０３で、選択エンティティＩＤによって構成されるツリーに必要なパス（キー配信ツリー構成のパス）を選択する。ステップＳ４３０４では、選択エンティティＩＤのリストに含まれる全てのパス選択が完了したか否かを判定し、完了するまで、ステップＳ４３０３においてパスを生成する。これは、複数のエンティティが選択された場合に、それぞれのパスを順次選択する処理を意味している。

【０２１６】選択エンティティＩＤのリストに含まれる全てのパス選択が完了すると、ステップＳ４３０５に進み、選択したパスと、選択エンティティによってのみ構成されるキー配信ツリー構造を構築する。

【０２１７】次に、ステップＳ４３０６において、ステップＳ４３０５で生成したツリー構造のノードキーの更新処理を行ない、更新ノードキーを生成する。さらに、ツリーを構成する選択エンティティのサブＥＫＢをケイパビリティ管理テーブルから取り出し、サブＥＫＢと、ステップＳ４３０６で生成した更新ノードキーとに基づいて選択エンティティのデバイスにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成する。このようにして生成した有効化キーブロック（ＥＫＢ）は、特定のケイパビリティを持つデバイスにおいてのみ利用、すなわち復号可能な有効化キーブロック（ＥＫＢ）となる。この有効化キーブロック（ＥＫＢ）で例えばコンテンツキーを暗号化して、そのコンテンツキーで特定プログラムに基づいて圧縮したコンテンツを暗号化してデバイスに提供することで、キー発行センター（ＫＤＣ）によって選択された特定の処理可能なデバイスにおいてのみコンテンツが利用される。

【０２１８】このようにキー発行センター（ＫＤＣ）は、ケイパビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キーブロック（ＥＫＢ）を生成する。従って、新たなエンティティが登録される場合には、その新規登録エンティティのケイパビリティを予め取得することが必要となる。このエンティティ新規登録に伴うケイパビリティ通知処理について図４４を用いて説明する。

【０２１９】図４４は、新規エンティティがキー配信ツリー構成に参加する場合のケイパビリティ通知処理シーケンスを示した図である。

【０２２０】新たにツリー構成中に追加される新規（子）エンティティ（Ｎ－Ｅｎ）は、上位（親）エンティティ（Ｐ－Ｅｎ）に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ（Ｐ－Ｅｎ）に送付する。

【０２２１】登録要求を受領した上位エンティティ（Ｐ－Ｅｎ）は、受領した新規（子）エンティティ（Ｎ－Ｅｎ）の公開鍵を証明書発行局（ＣＡ：Certificate Authority）に転送し、ＣＡの署名を付加した新規（子）エンティティ（Ｎ－Ｅｎ）の公開鍵を受領する。これらの手続きは、上位エンティティ（Ｐ－Ｅｎ）と新規（子）エンティティ（Ｎ－Ｅｎ）との相互認証の手続きとして行われる。

【０２２２】これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ（Ｐ－Ｅｎ）は、新規（子）エンティティ（Ｎ－Ｅｎ）の登録を許可し、新規（子）エンティティ（Ｎ－Ｅｎ）のノードキーを新規（子）エンティティ（Ｎ－Ｅｎ）に送信する。このノードキーは、上位エンティティ（Ｐ－Ｅｎ）

の末端ノードの１つのノードキーであり、かつ、新規（子）エンティテイ（Ｎ－Ｅｎ）の頂点ノード、すなわちサブルートキーに対応する。

【０２２３】このノードキー送信が終了すると、新規（子）エンティテイ（Ｎ－Ｅｎ）は、新規（子）エンティテイ（Ｎ－Ｅｎ）のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティテイ内の有効化キーブロック（サブＥＫＢ）を生成する。一方、上位エンティテイ（Ｐ－Ｅｎ）も、新規（子）エンティテイ（Ｎ－Ｅｎ）の追加により、有効化する末端ノードを追加した上位エンティテイ（Ｐ－Ｅｎ）内のサブＥＫＢを生成する。

【０２２４】新規（子）エンティテイ（Ｎ－Ｅｎ）は、新規（子）エンティテイ（Ｎ－Ｅｎ）内のノードキー、リーフキーによって構成されるサブＥＫＢを生成すると、これを上位エンティテイ（Ｐ－Ｅｎ）に送信し、さらに、自己のエンティテイで管理するデバイスについてのケイパビリティ情報を上位エンティテイに通知する。

【０２２５】新規（子）エンティテイ（Ｎ－Ｅｎ）からサブＥＫＢおよびケイパビリティ情報を受信した上位エンティテイ（Ｐ－Ｅｎ）は、受信したサブＥＫＢとケイパビリティ情報と、上位エンティテイ（Ｐ－Ｅｎ）の更新したサブＥＫＢとをキー発行センター（ＫＤＣ：Key Distribute Center）に送信する。

【０２２６】キー発行センター（ＫＤＣ）は、受領したエンティテイのサブＥＫＢおよびケイパビリティ情報とを図４２で説明したケイパビリティ管理テーブルに登録し、ケイパビリティ管理テーブルを更新する。キー発行センター（ＫＤＣ）は、更新したケイパビリティ管理テーブルに基づいて、様々な態様のＥＫＢ、すなわち特定のケイパビリティを持つエンティテイあるいはデバイスのみが復号可能なＥＫＢを生成することが可能となる。

【０２２７】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２２８】

【発明の効果】以上、説明したように、本発明の情報処理システムおよび方法によれば、複数のデバイスをリーフとして構成したツリーのルートからリーフまでのパス上のルート、ノード、およびリーフに各々キーを対応付けたキーツリーをデバイスのデータ処理能力としてのケイパビリティに基づいて区分したサブツリーを設定し、それぞれのサブツリーの管理主体であるエンティテイにおいて、エンティテイ内で有効なサブ有効化キーブロック（サブＥＫＢ）を生成するとともに、キー発行センター（ＫＤＣ）において、エンティテイのケイパビリティ情報を管理して、共通のケイパビリティを持つエンティテイにおいてのみ復号可能な有効化キーブロック（ＥＫＢ）を生成する構成としたので、特定のデバイスにおいてのみ処理可能なデータを、そのデバイスにおいてのみ復号可能なデータとして提供することが可能となる。

【０２２９】さらに、本発明の情報処理システムおよび方法によれば、キー発行センター（ＫＤＣ）は、複数のエンティテイ各々の識別子、ケイパビリティ情報、サブ有効化キーブロック（サブＥＫＢ）情報とを対応付けたケイパビリティ管理テーブルに基づいて、デバイスに対する配信データの処理可能なエンティテイを選択して、様々なケイパビリティに応じた様々なＥＫＢの生成が可能となる。

【０２３０】さらに、本発明の情報処理システムおよび方法によれば、エンティテイでのデバイスあるいはエンティテイのリボーク処理が実行可能であり、一括したデバイス管理の場合のデバイス増大にともなう処理量の増加が防止される。

【０２３１】さらに、本発明の情報処理システムおよび方法によれば、各エンティティの末端ノードにリザーブノードを設定する構成としたので、管理デバイスまたは管理エンティテイの増加にも対応可能となる。

【図面の簡単な説明】

【図１】本発明の情報処理システムの構成例を説明する図である。

【図２】本発明の情報処理システムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

【図３】本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図４】本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図５】本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

【図６】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

【図７】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

【図８】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図９】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

【図１０】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）とコンテンツを記録媒体に格納し

た場合の対応について説明する図である。

【図１１】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキーを送付する処理を従来の送付処理と比較した図である。

【図１２】本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

【図１３】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その１）である。

【図１４】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その２）である。

【図１５】本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

【図１６】本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キーブロック（ＥＫＢ）と、コンテンツキーを併せて配信する処理を示す図である。

【図１７】本発明の情報処理システムにおいて有効化キーブロック（ＥＫＢ）と、暗号化プログラムデータを併せて配信する処理を示す図である。

【図１８】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）の生成に使用するＭＡＣ値生成例を示す図である。

【図１９】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、ＩＣＶ生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その１）である。

【図２０】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）と、ＩＣＶ生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その２）である。

【図２１】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）をメディアに格納した場合のコピー防止機能を説明する図である。

【図２２】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ＩＣＶ）をコンテンツ格納媒体と別に管理する構成を説明する図である。

【図２３】本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

【図２４】本発明の情報処理システムにおける簡略化有効化キーブロック（ＥＫＢ）の生成過程を説明する図である。

【図２５】本発明の情報処理システムにおける有効化キーブロック（ＥＫＢ）の生成過程を説明する図である。

【図２６】本発明の情報処理システムにおける簡略化有効化キーブロック（ＥＫＢ）を説明する図である。

【図２７】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成について説明する図である。

【図２８】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成の詳細について説明する図である。

【図２９】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成について説明する図である。

【図３０】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのリザーブノードについて説明する図である。

【図３１】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成での新規エンティテイ登録処理シーケンスについて説明する図である。

【図３２】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成での新規エンティテイと上位エンティテイの関係について説明する図である。

【図３３】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成で用いるサブＥＫＢについて説明する図である。

【図３４】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのデバイスリボーク処理について説明する図である。

【図３５】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのデバイスリボーク処理シーケンスについて説明する図である。

【図３６】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのデバイスリボーク時の更新サブＥＫＢについて説明する図である。

【図３７】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのエンティテイリボーク処理について説明する図である。

【図３８】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのエンティテイリボーク処理シーケンスについて説明する図である。

【図３９】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのリボークエンティテイと上位エンティテイの関係について説明する図である。

【図４０】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのケイパビリテイ設定について説明する図である。

【図４１】本発明の情報処理システムにおける階層ツリー構造のエンティテイ管理構成でのケイパビリテイ設定について説明する図である。

【図４２】本発明の情報処理システムにおけるキー発行

センター（ＫＤＣ）の管理するケイパビリティ管理テーブル構成を説明する図である。

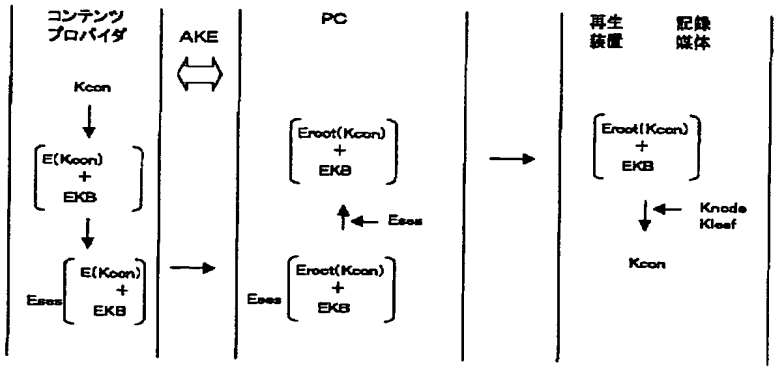
【図４３】本発明の情報処理システムにおけるキー発行センター（ＫＤＣ）の管理するケイパビリティ管理テーブルに基づくＥＫＢ生成処理フロー図である。

【図４４】本発明の情報処理システムにおける新規エンティティ登録時のケイパビリティ通知処理を説明する図である。

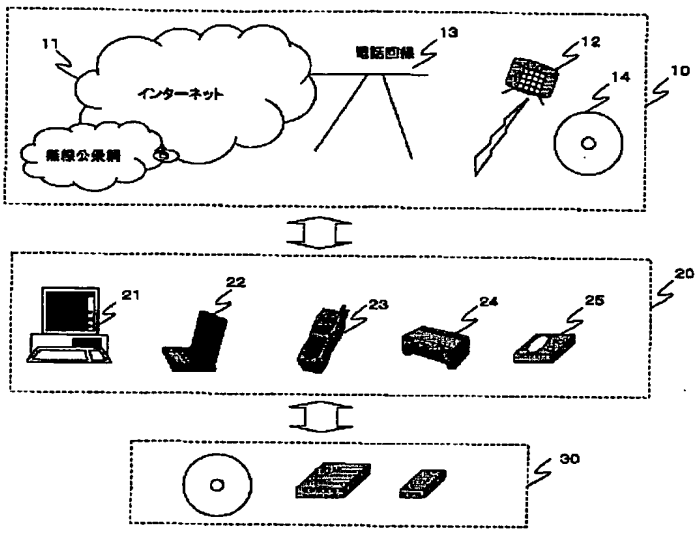
【符号の説明】

１０　コンテンツ配信側
１１　インターネット
１２　衛星放送
１３　電話回線
１４　メディア
２０　コンテンツ受信側
２１　パーソナルコンピュータ（ＰＣ）
２２　ポータブルデバイス（ＰＤ）
２３　携帯電話、ＰＤＡ
２４　記録再生器
２５　再生専用器
３０　メディア
１００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　ドライブ
１９５　記録媒体
６０１　バージョン
６０２　デプス
６０３　データポインタ
＊６０４　タグポインタ
６０５　署名ポインタ
６０６　データ部
６０７　タグ部
６０８　署名
１１０１　記録デバイス
２３０１　ルートキー
２３０２　ノードキー
２３０３　リーフキー
２３０４　カテゴリノード
２３０６　サブカテゴリノード
２７０１　エンティティ
２７０２　サブルート
２８１１，２８５１　サブルート
２８１２，２８５２　エンティティ末端ノード
２９０１，２９０２　エンティティ
２９５０　リザーブノード
２９７０　管理末端ノード
３０１１，３０１２，３０１３　エンティティ
３０２１，３０２２，３０２３　リザーブノード
３２０１　末端ノード
３２０２　頂点ノード
３３０１，３３０２　末端ノード
３３０３　新規エンティティ追加末端ノード
３４１０，３４２０，３４３０　エンティティ
３４１１，３４２１，３４３１　サブルート
３４３２　リボークデバイスノード
３６０１　末端ノード
３７１０，３７２０，３７３０　エンティティ
３７１１，３７２１，３７３１　サブルート
３９０１　末端ノード
３９０２　頂点ノード（サブルートノード）
４００１～４００５　エンティティ
４０２１，４０２２，４０２３　エンティティ
４１０１～４１０５　エンティティ
＊

【図１６】



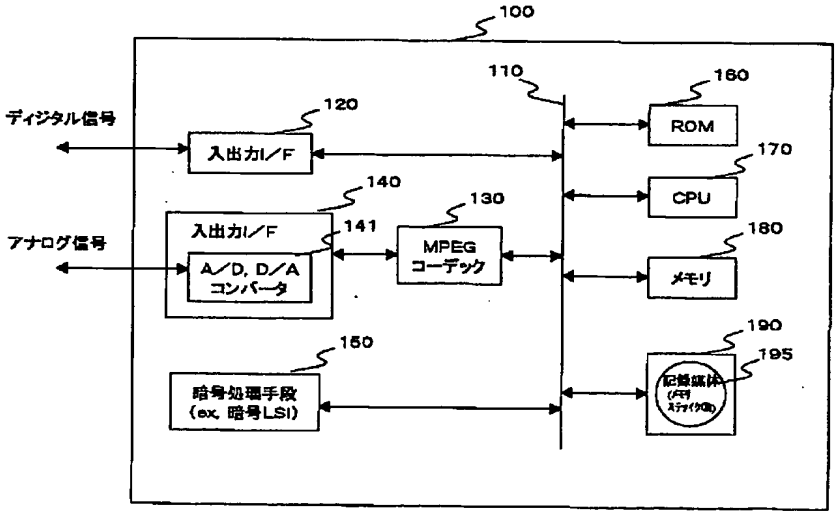
【図１】


11
インターネット
無線公衆網
13
電話回線
12
14
10
21
22
23
24
25
20
30

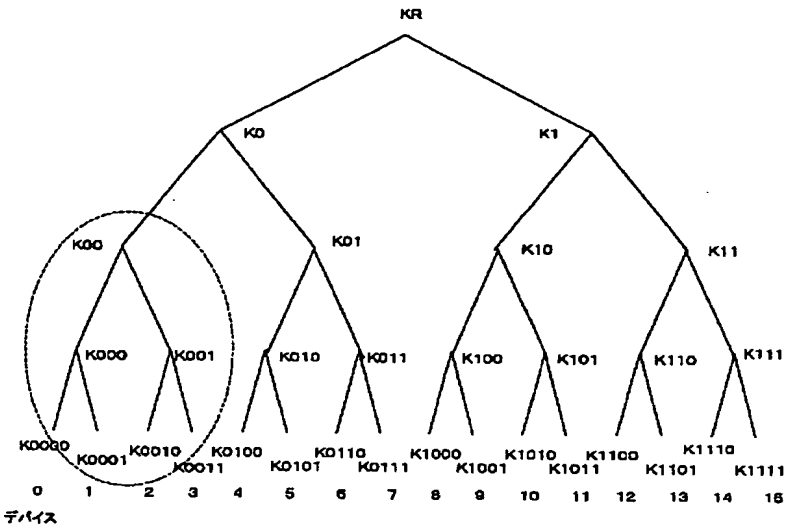
【図１０】


格納コンテンツ
コンテンツ:C1
コンテンツ:C2
コンテンツ:C3
コンテンツ:C4
格納EKB
EKB_M
対応付けデータ
<コンテンツ:C1 EKB_1>
<コンテンツ:C2 EKB_2>
<コンテンツ:C3 EKB_M>
<コンテンツ:C4 EKB_M>
記録媒体

【図２】


100
110
160
ROM
120
ディジタル信号
入出力I/F
170
CPU
140
130
入出力I/F
141
MPEG
コーデック
アナログ信号
A/D, D/A
コンバータ
180
メモリ
190
150
195
暗号処理手段
(ex. 暗号LSI)

【図３】



【図４】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

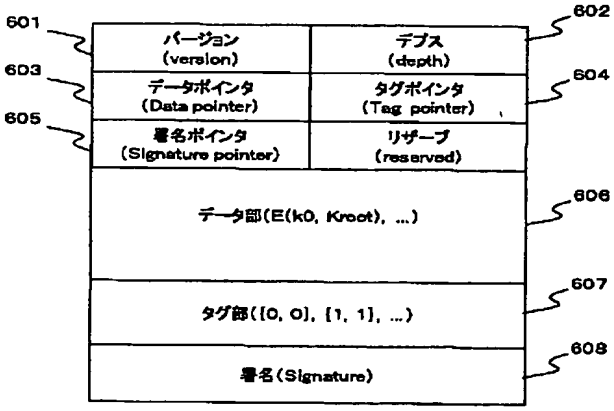
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

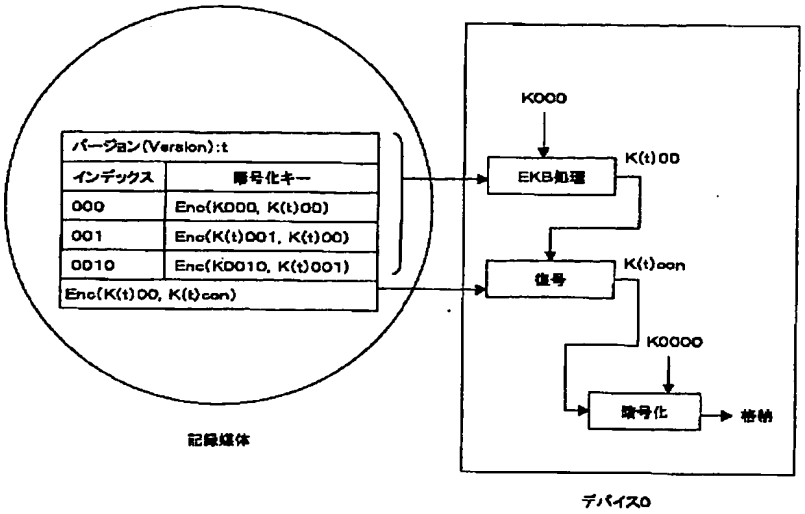
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

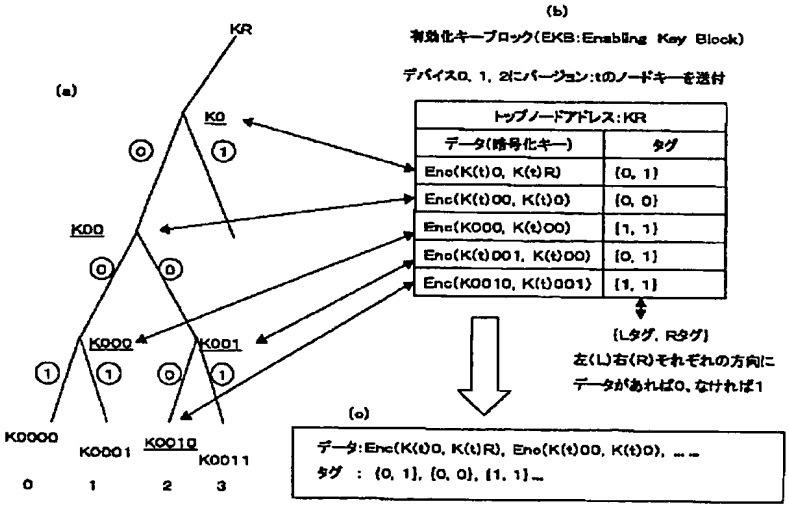
【図６】



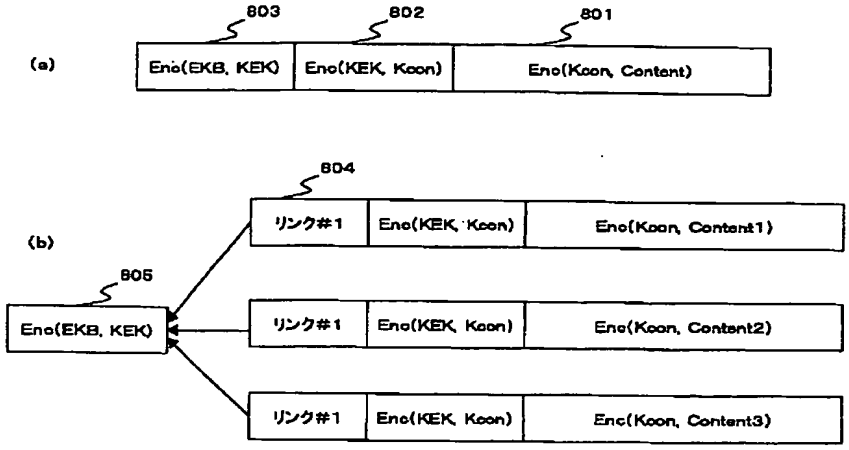
【図５】


バージョン(Version):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
記録媒体
K000
EKB処理
K(t)00
復号
K(t)con
K0000
暗号化
格納
デバイス0

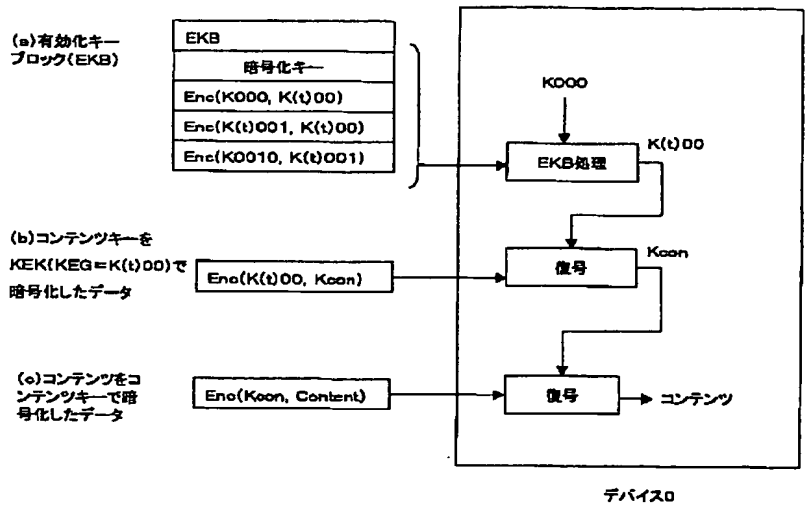
【図７】


(a)
KR
K0
K00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
[Lタグ, Rタグ]
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
タグ : {0, 1}, {0, 0}, {1, 1}…

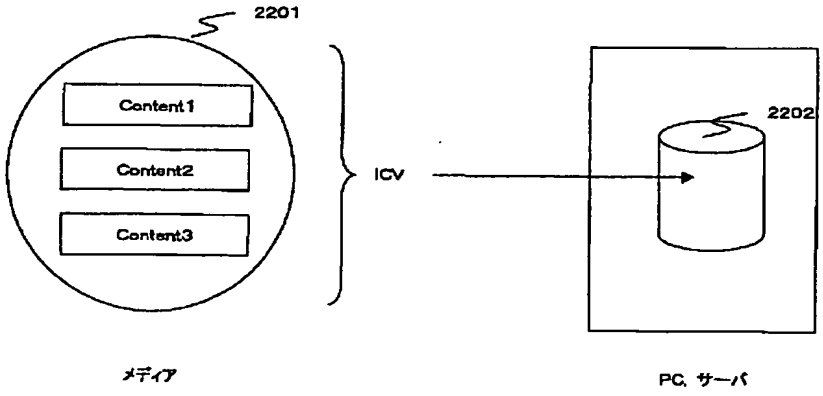
【図８】


803
802
801
(a)
Enc(EKB, KEK)
Enc(KEK, Kcon)
Enc(Kcon, Content)
804
(b)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
805
Enc(EKB, KEK)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content2)
リンク#1
Enc(KEK, Kcon)
Enc(Kcon, Content3)

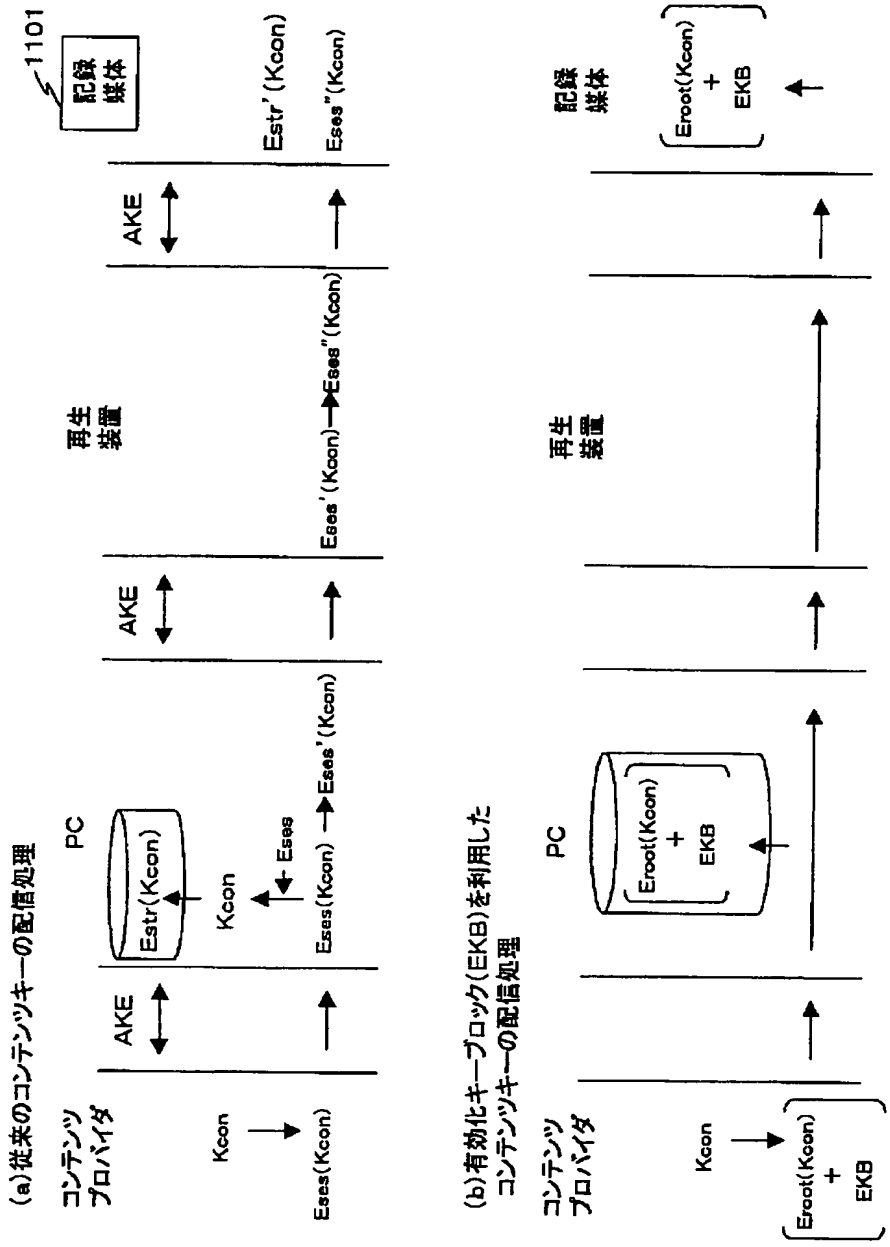
【図９】


(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K000
EKB処理
K(t)00
(b)コンテンツキーをKEK(KEG=K(t)00)で暗号化したデータ
Enc(K(t)00, Kcon)
復号
Kcon
(c)コンテンツをコンテンツキーで暗号化したデータ
Enc(Kcon, Content)
復号
コンテンツ
デバイス0

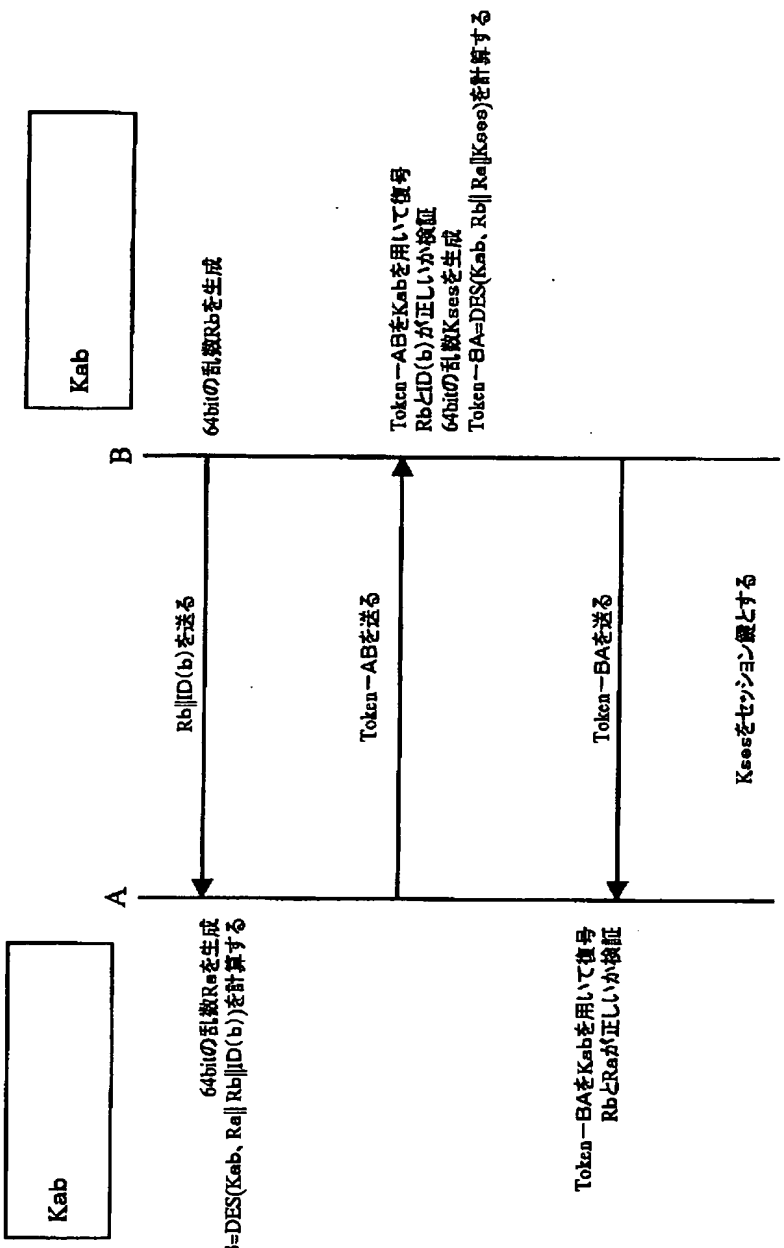
【図２２】


2201
Content1
Content2
Content3
ICV
2202
メディア
PC, サーバ

【図１１】

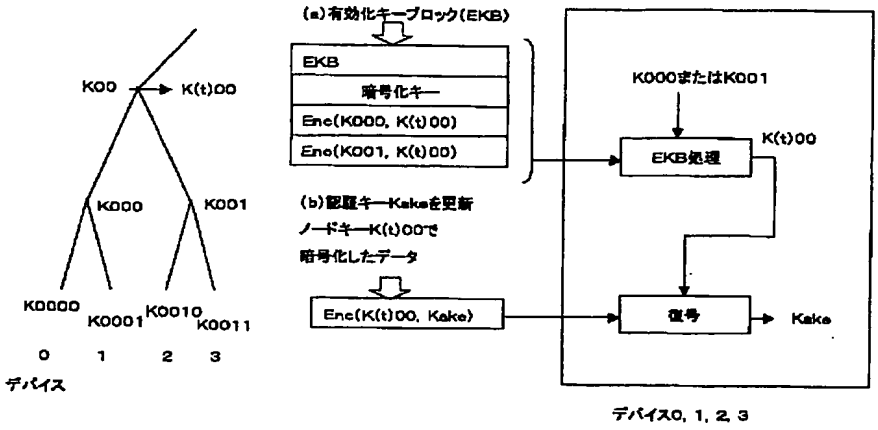

(a)従来のコンテンツキーの配信処理
コンテンツプロバイダ
PC
再生装置
記録媒体
1101
AKE
Estr(Kcon)
Kcon
Esas
Esas(Kcon)
Esas'(Kcon)
Estr'(Kcon)
Esas"(Kcon)
(b)有効化キーブロック(EKB)を利用したコンテンツキーの配信処理
Eroot(Kcon)
+
EKB

【図１２】

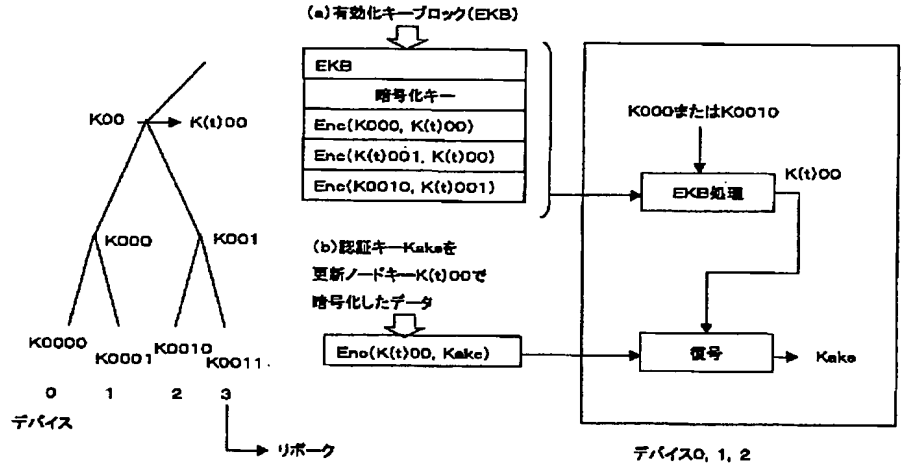


ISO/IEC 9798-2　対称鍵暗号技術を用いた相互認証および鍵共有方式

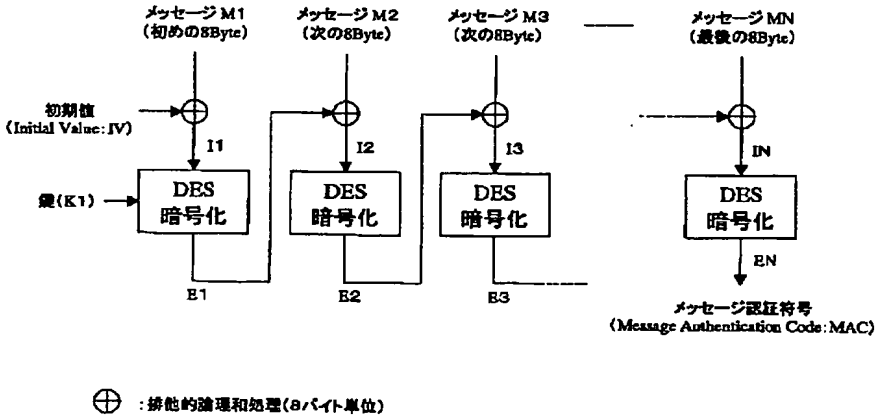
【図１３】



【図１４】

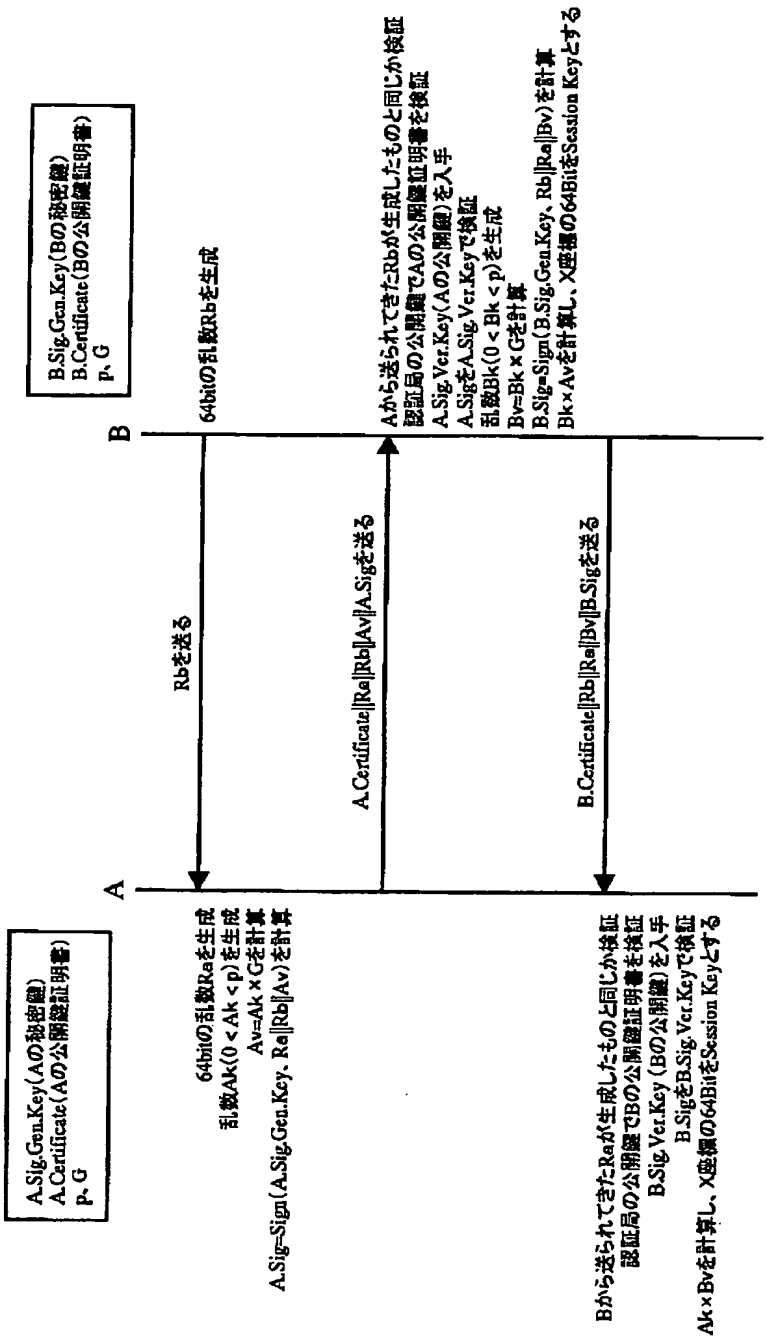


【図１８】



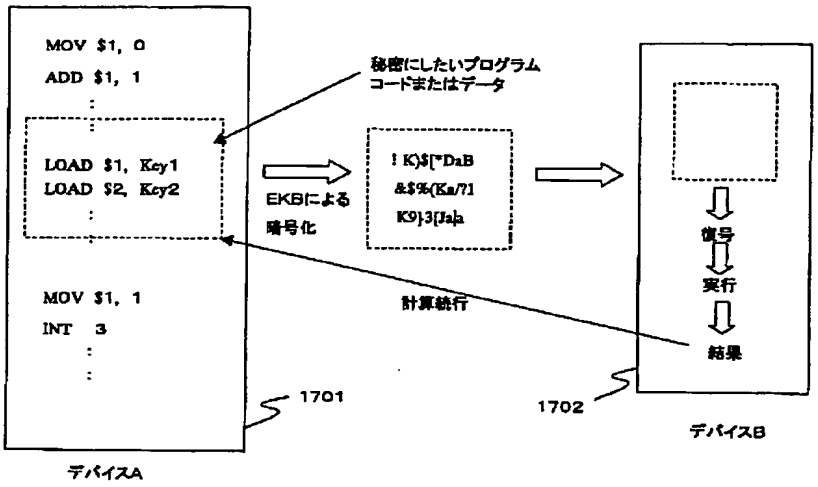
⊕ :排他的論理和処理(8バイト単位)

【図１５】

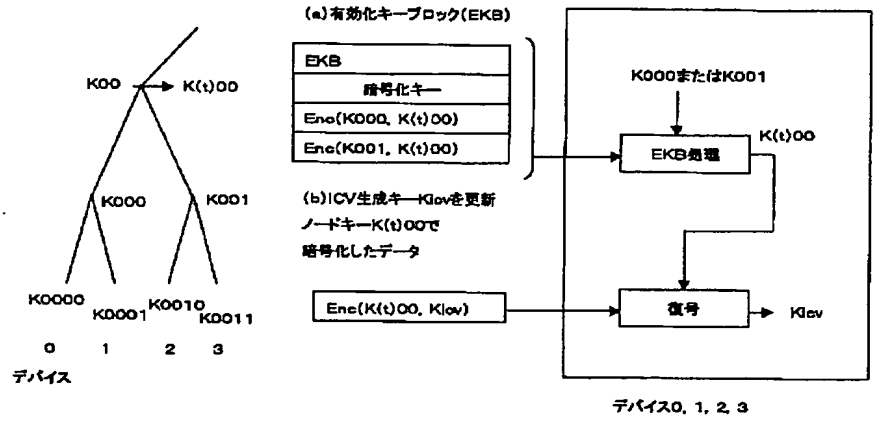


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

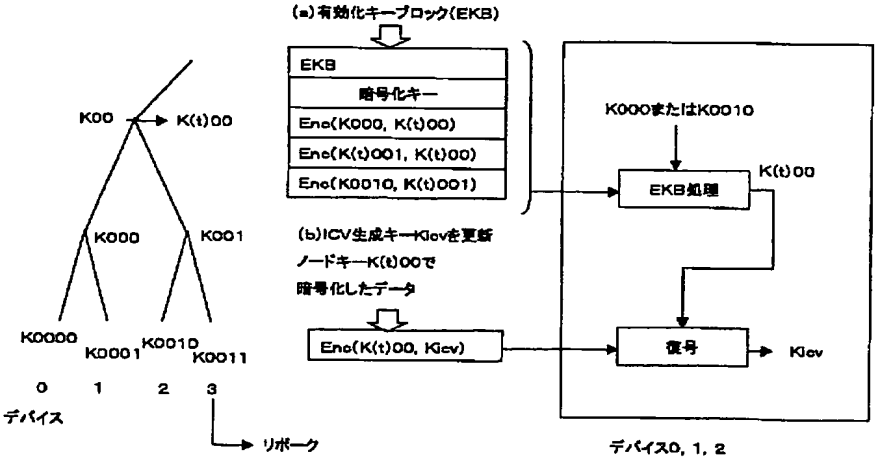
【図１７】


MOV $1, 0
ADD $1, 1
LOAD $1, Key1
LOAD $2, Key2
MOV $1, 1
INT 3
秘密にしたいプログラム
コードまたはデータ
EKBによる
暗号化
! K)$["DaB
&$%(Ka/?1
K9}3[Ja|a
復号
実行
結果
計算続行
1701
1702
デバイスA
デバイスB

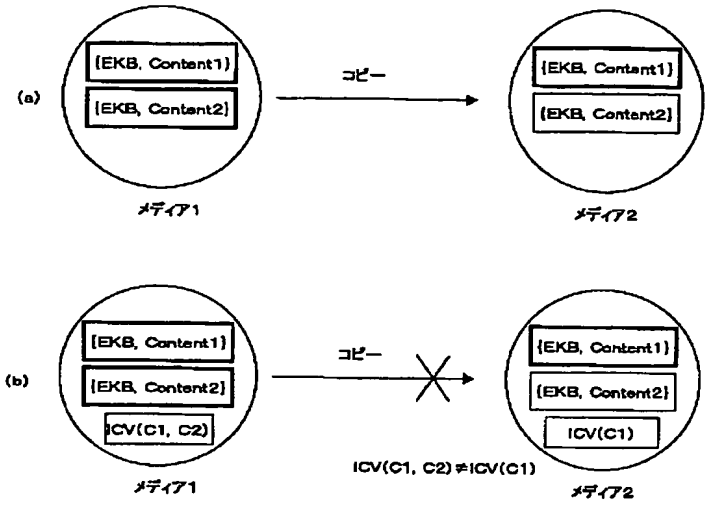
【図１９】


(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K001, K(t)00)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0 1 2 3
デバイス
(b)ICV生成キーKicvを更新
ノードキーK(t)00で
暗号化したデータ
Enc(K(t)00, Kicv)
K000またはK001
EKB処理
K(t)00
復号
Kicv
デバイス0, 1, 2, 3

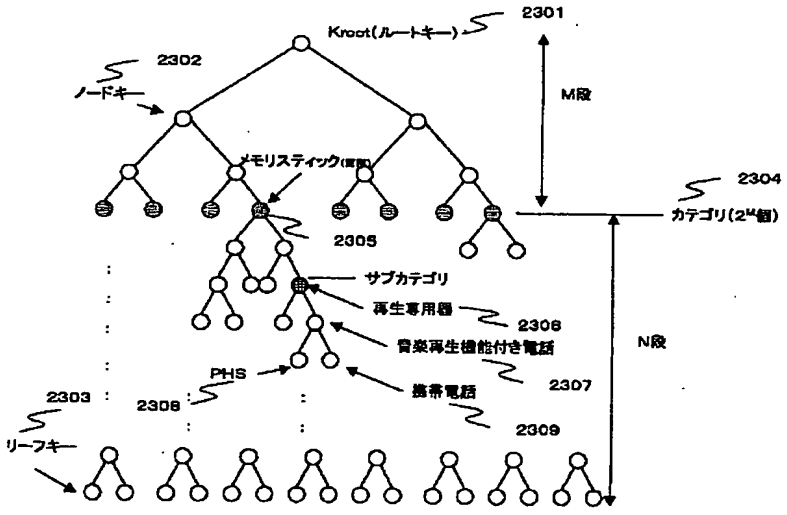
【図２０】


(a)有効化キーブロック(EKB)
EKB
暗号化キー
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0 1 2 3
デバイス
リボーク
(b)ICV生成キーKicvを更新
ノードキーK(t)00で
暗号化したデータ
Enc(K(t)00, Kicv)
K000またはK0010
EKB処理
K(t)00
復号
Kicv
デバイス0, 1, 2

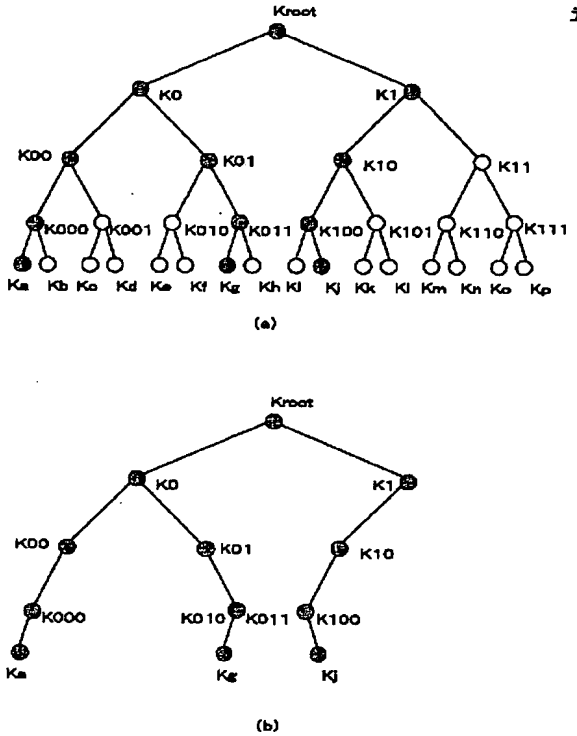
【図２１】


(a)
{EKB, Content1}
{EKB, Content2}
コピー
{EKB, Content1}
{EKB, Content2}
メディア1
メディア2
(b)
{EKB, Content1}
{EKB, Content2}
ICV(C1, C2)
コピー
{EKB, Content1}
{EKB, Content2}
ICV(C1)
ICV(C1, C2)≠ICV(C1)
メディア1
メディア2

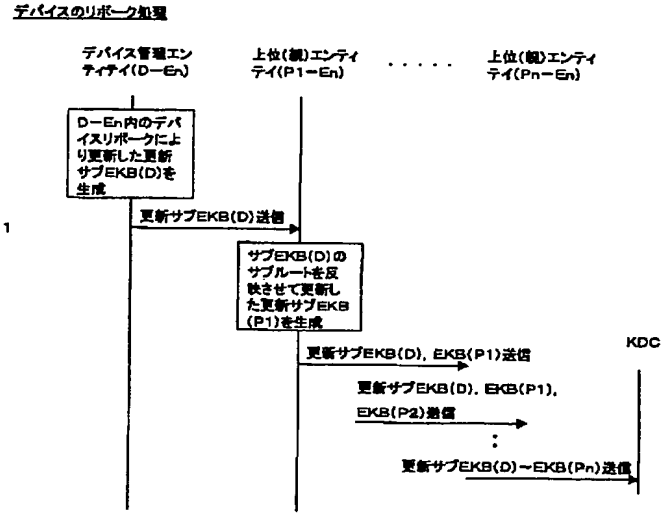
【図２３】


Kroot(ルートキー)
2301
2302
ノードキー
M段
メモリスティック
2304
カテゴリ(2^M個)
2305
サブカテゴリ
再生専用器
2306
音楽再生機能付き電話
N段
PHS
2307
携帯電話
2303
2308
2309
リーフキー

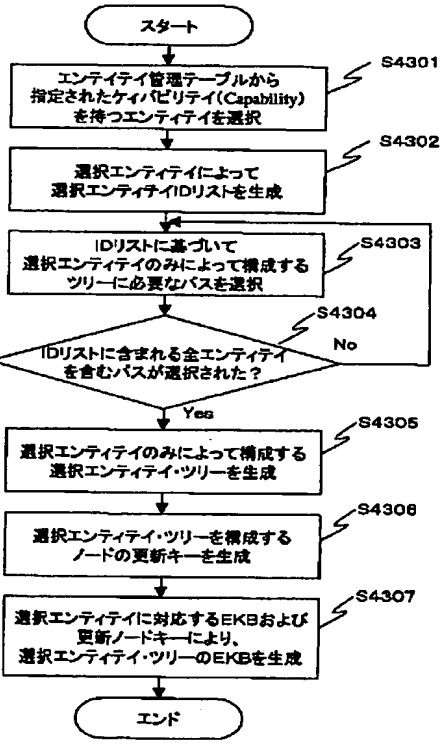
【図２４】



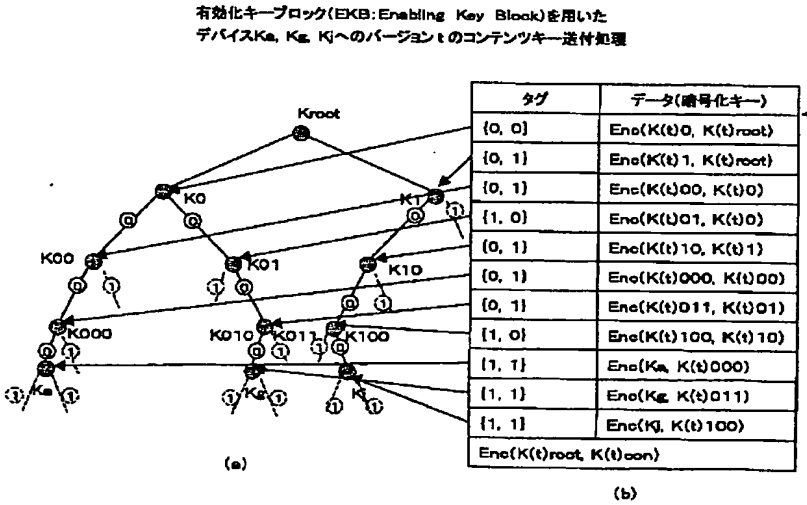
【図３５】



【図４３】

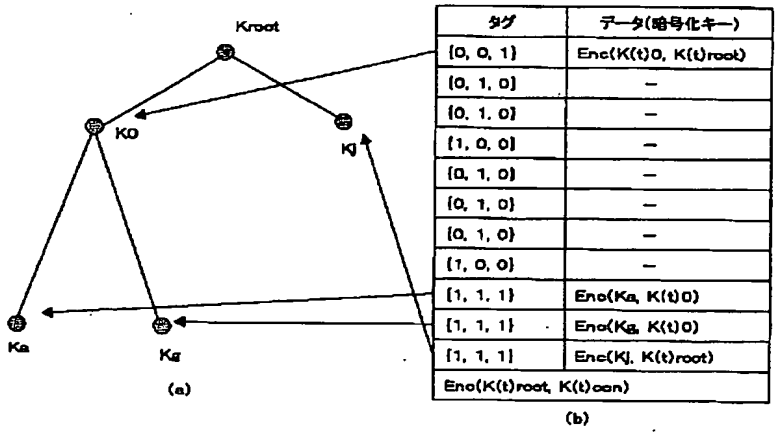


【図２５】



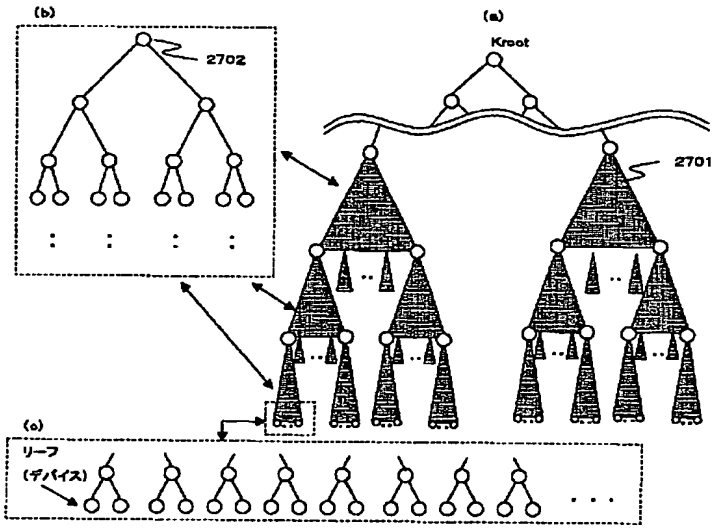
【図２６】

簡略化した有効化キーブロック(EKB:Enabling Key Block)を用いた
デバイスKa, Kg, Kjへのバージョンｔのコンテンツキー送付処理

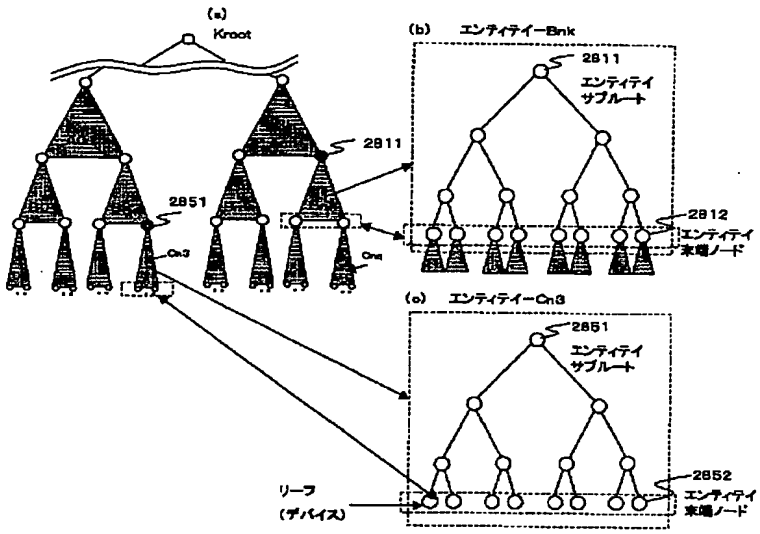


タグ	データ(暗号化キー)
{0, 0, 1}	Enc(K(t)0, K(t)root)
{0, 1, 0}	–
{0, 1, 0}	–
{1, 0, 0}	–
{0, 1, 0}	–
{0, 1, 0}	–
{0, 1, 0}	–
{1, 0, 0}	–
{1, 1, 1}	Enc(Ka, K(t)0)
{1, 1, 1}	Enc(Kg, K(t)0)
{1, 1, 1}	Enc(Kj, K(t)root)
Enc(K(t)root, K(t)con)	

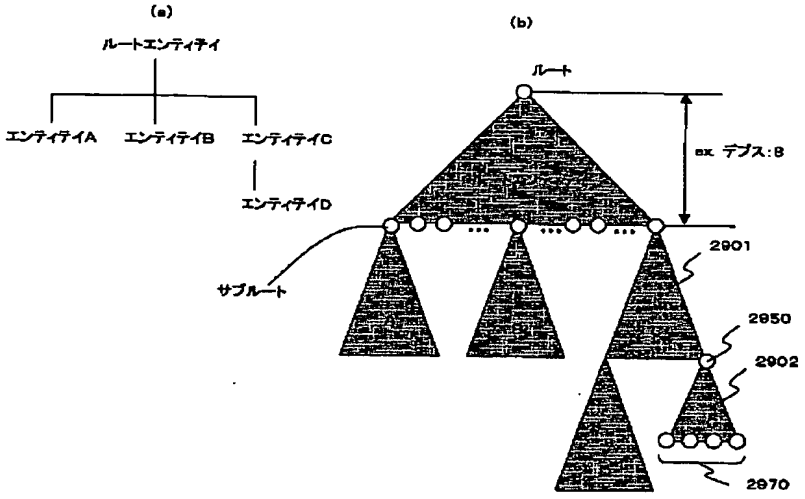
【図２７】



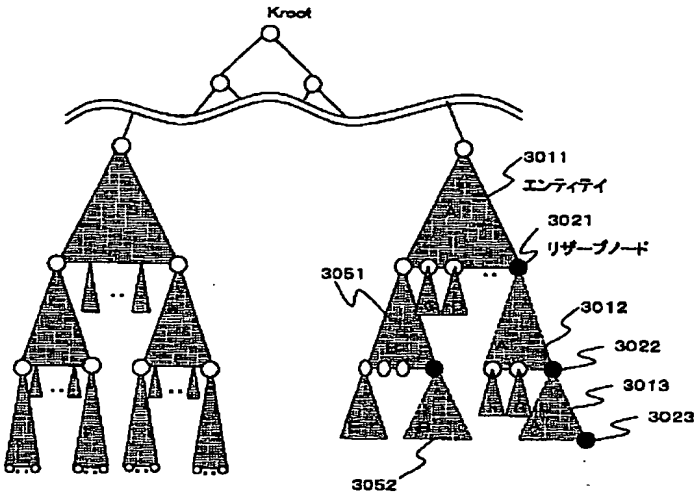
【図２８】


(a)
Kroot
2811
2851
Cn3
Cn1
(b) エンティティーBnk
2811
エンティティ
サブルート
2812
エンティティ
末端ノード
(c) エンティティーCn3
2851
エンティティ
サブルート
2852
エンティティ
末端ノード
リーフ
(デバイス)

【図２９】

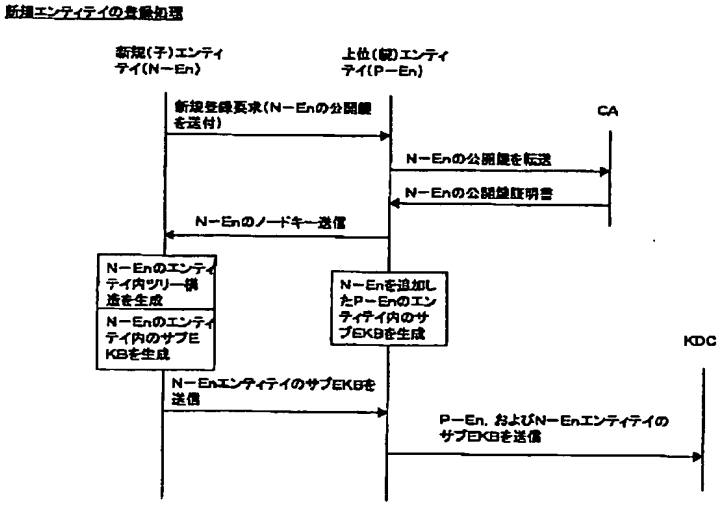

(a)
ルートエンティティ
エンティティA
エンティティB
エンティティC
エンティティD
(b)
ルート
ex. デプス:8
サブルート
2901
2950
2902
2970

【図３０】

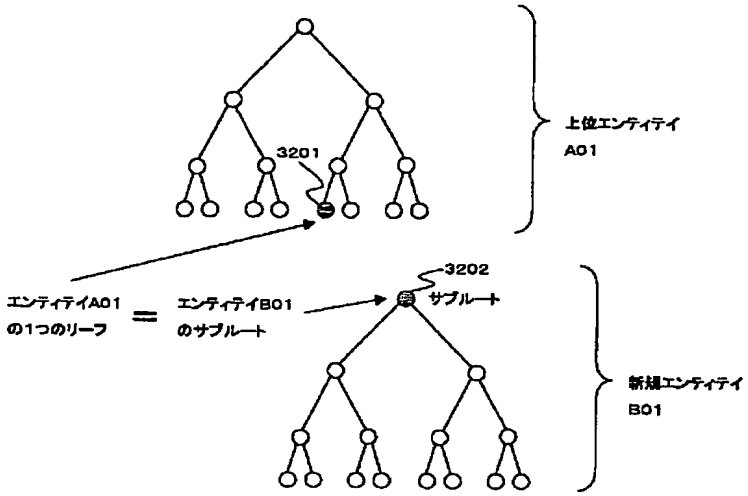


リザーブノードの構成

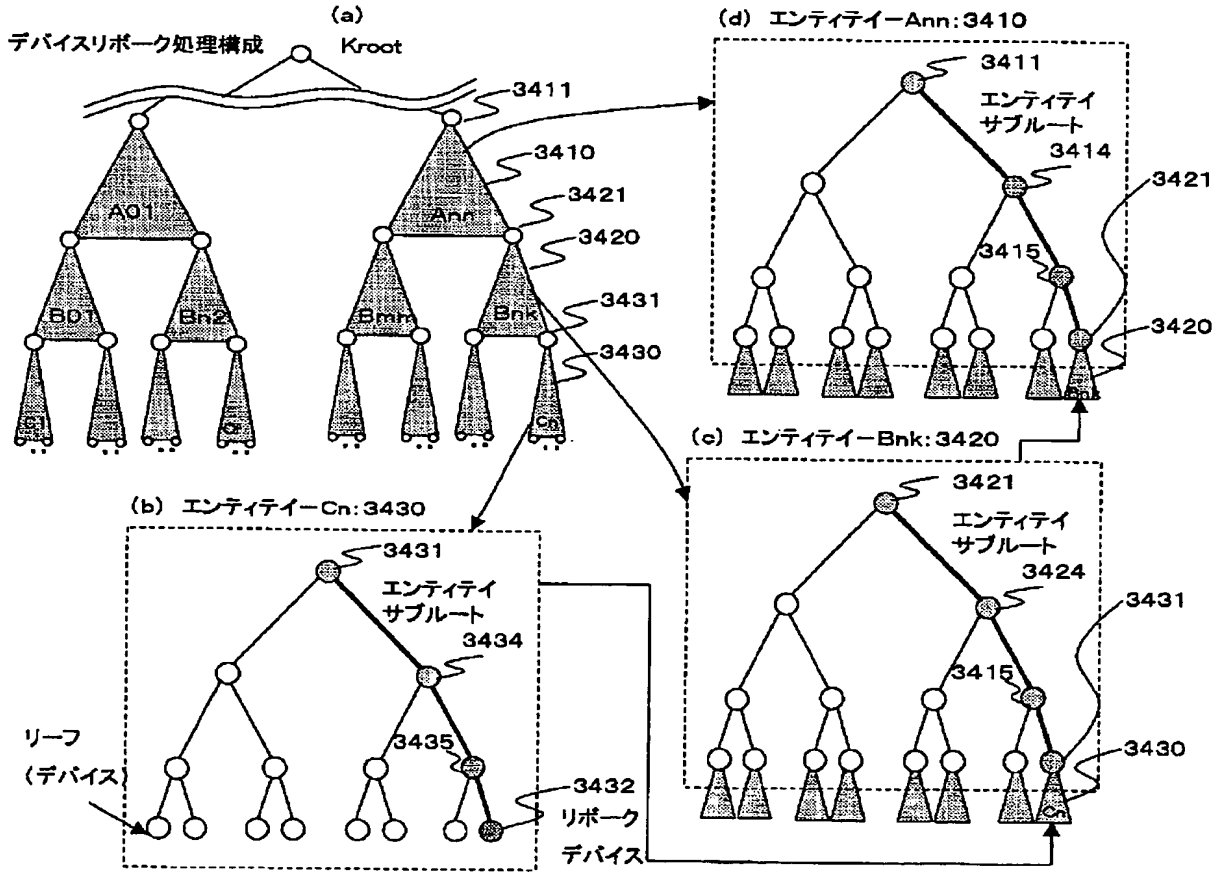
【図３１】



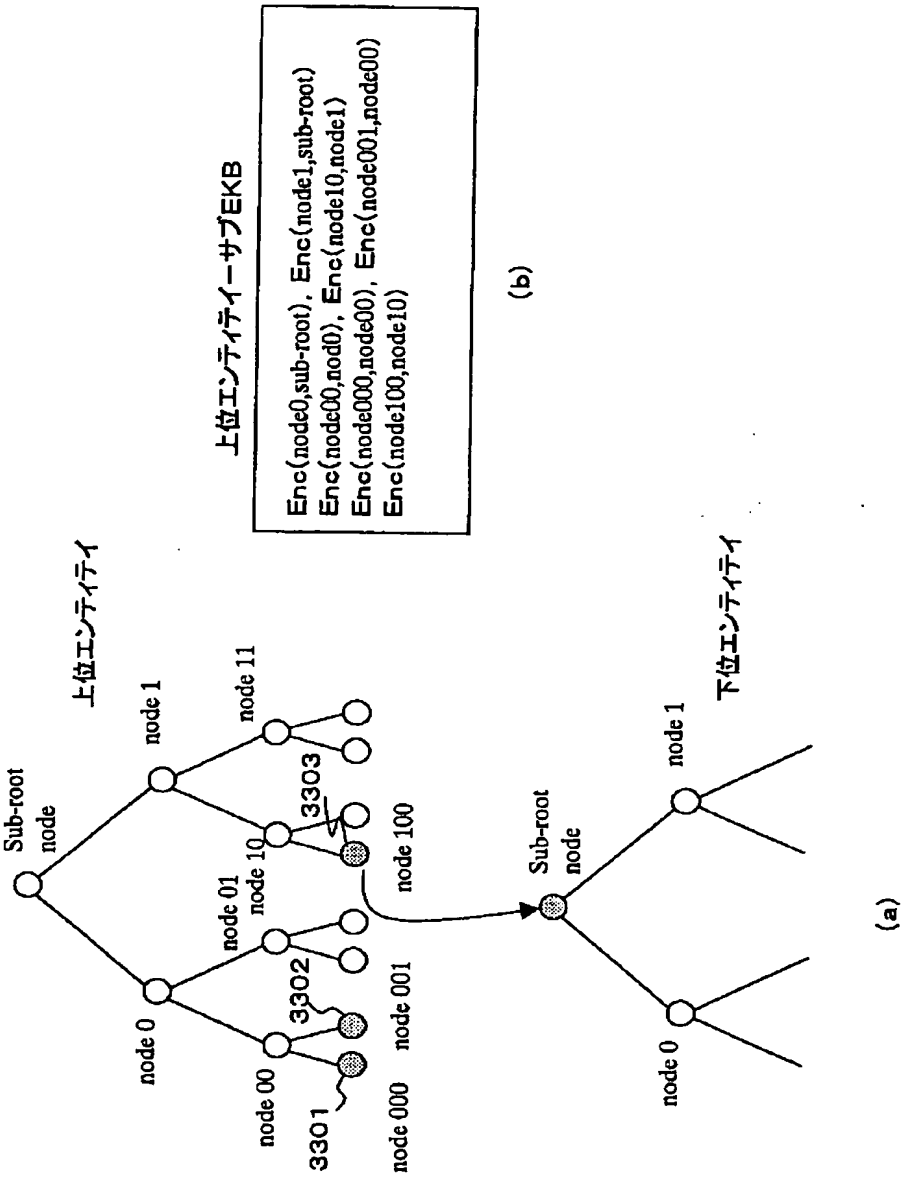
【図３２】


3201
上位エンティティ
A01
エンティティA01
の1つのリーフ
=
エンティティB01
のサブルート
3202
サブルート
新規エンティティ
B01

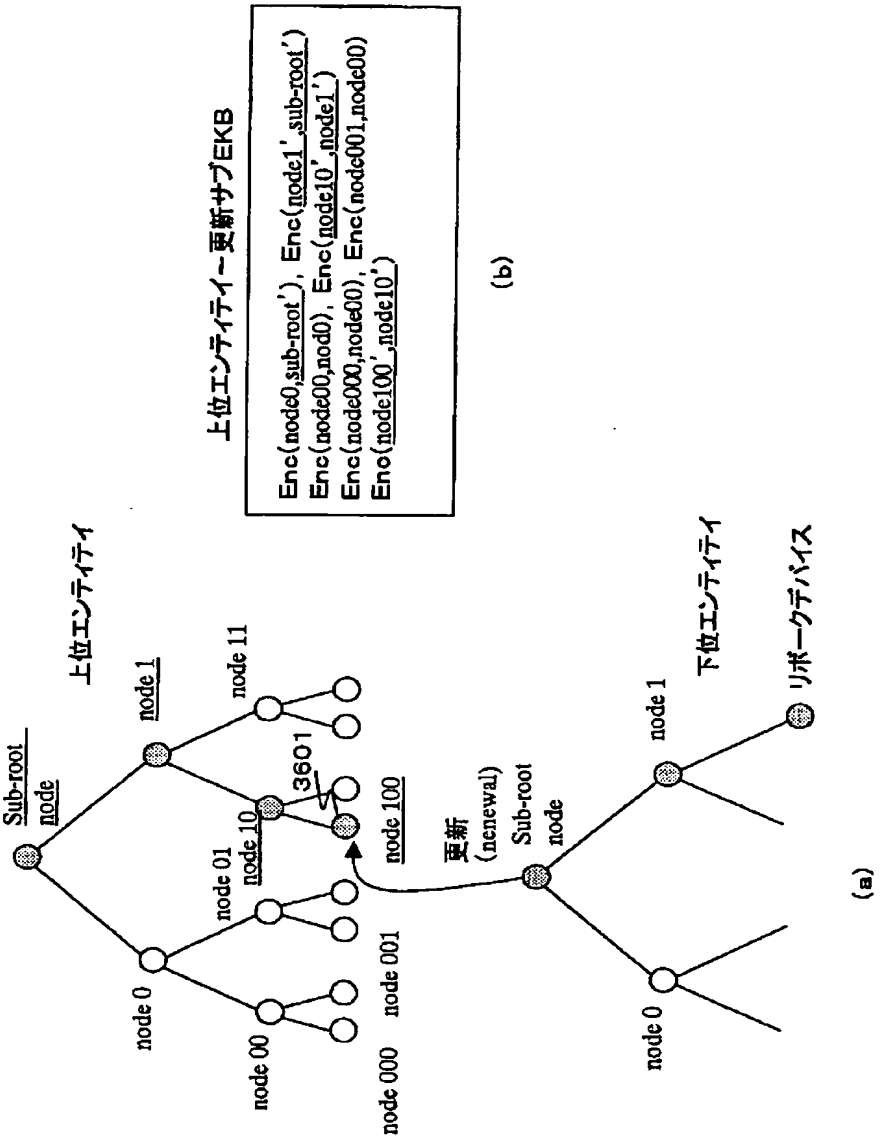
【図３４】


(a)
デバイスリポーク処理構成
Kroot
3411
3410
3421
3420
3431
3430
A01
Ann
Bn1
Bn2
Bnm
Bnk
C1
C2
Cn
(b) エンティティーCn:3430
3431
エンティティ
サブルート
3434
3435
3432
リポーク
デバイス
リーフ
(デバイス)
(c) エンティティーBnk:3420
3421
エンティティ
サブルート
3424
3415
3431
3430
(d) エンティティーAnn:3410
3411
エンティティ
サブルート
3414
3415
3421
3420

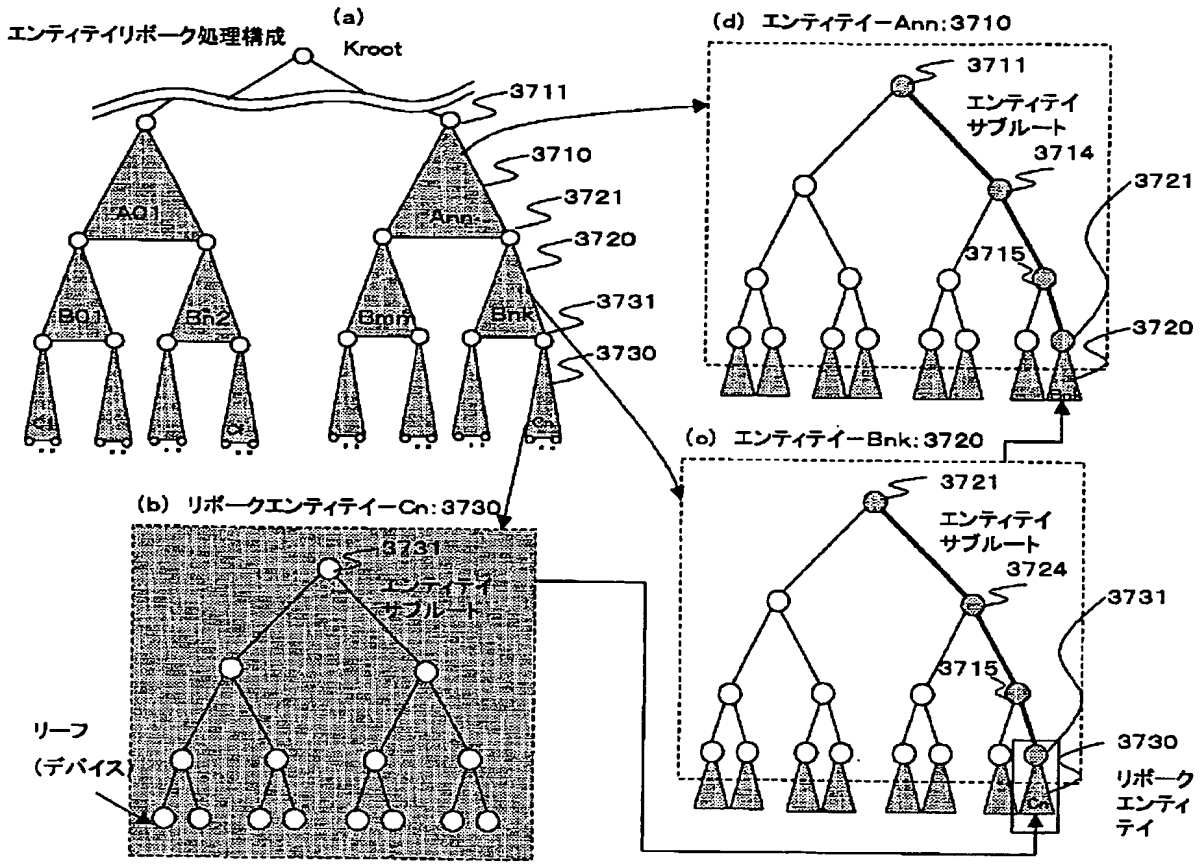
【図３３】


上位エンティティ
Sub-root node
node 0
node 1
node 00
node 01
node 10
node 11
node 000
node 001
node 100
3301
3302
3303
(a)
下位エンティティ
Sub-root node
node 0
node 1
(b)
上位エンティティーサブEKB
Enc(node0,sub-root), Enc(node1,sub-root)
Enc(node00,node0), Enc(node10,node1)
Enc(node000,node00), Enc(node001,node00)
Enc(node100,node10)

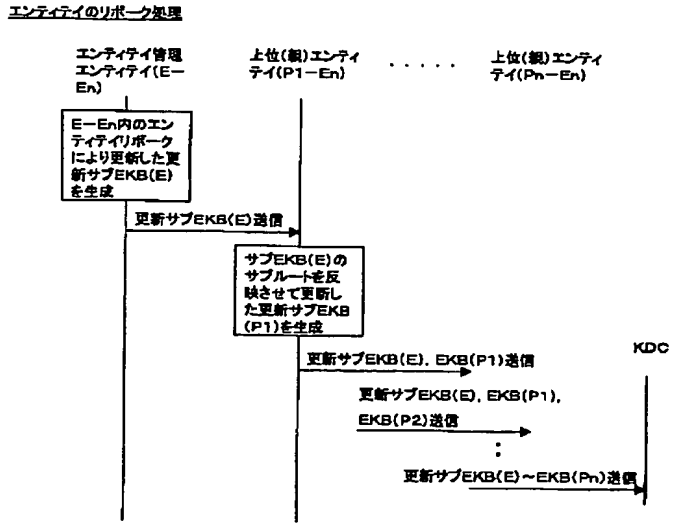
【図３６】


上位エンティティ
Sub-root node
node 1
node 11
node 0
node 01
node 10
node 00
node 000
node 001
node 100
3601
更新 (renewal) Sub-root node
node 1
node 0
下位エンティティ
リポークデバイス
(a)
上位エンティティ～更新サブEKB
Enc(node0,sub-root'), Enc(node1',sub-root')
Enc(node00,nod0), Enc(node10',node1')
Enc(node000,node00), Enc(node001,node00)
Eno(node100',node10')
(b)

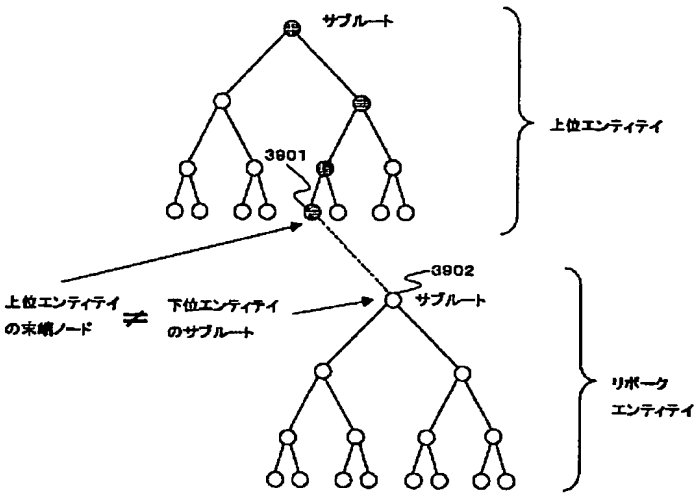
【図３７】


エンティティリポーク処理構成
(a)
Kroot
3711
3710
3721
3720
3731
3730
An
Bn1
Bn2
Bnm
Bnk
C1
C2
Cn
(b) リポークエンティティーCn:3730
3731
エンティティ
サブルート
リーフ
(デバイス)
(d) エンティティーAnn:3710
3711
エンティティ
サブルート
3714
3721
3715
3720
(e) エンティティーBnk:3720
3721
エンティティ
サブルート
3724
3731
3715
3730
Cn
リポーク
エンティ
テイ

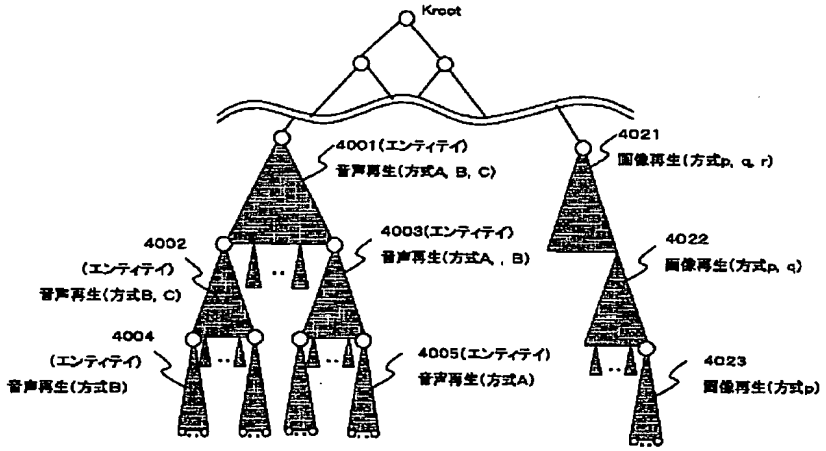
【図３８】


エンティティのリポーク処理
エンティティ情報
エンティティ(E－En)
上位(親)エンティティ(P1－En)
上位(親)エンティティ(Pn－En)
E－En内のエンティティリポークにより更新した更新サブEKB(E)を生成
更新サブEKB(E)送信
サブEKB(E)のサブルートを反映させて更新した更新サブEKB(P1)を生成
KDC
更新サブEKB(E)，EKB(P1)送信
更新サブEKB(E)，EKB(P1)，EKB(P2)送信
更新サブEKB(E)～EKB(Pn)送信

【図３９】

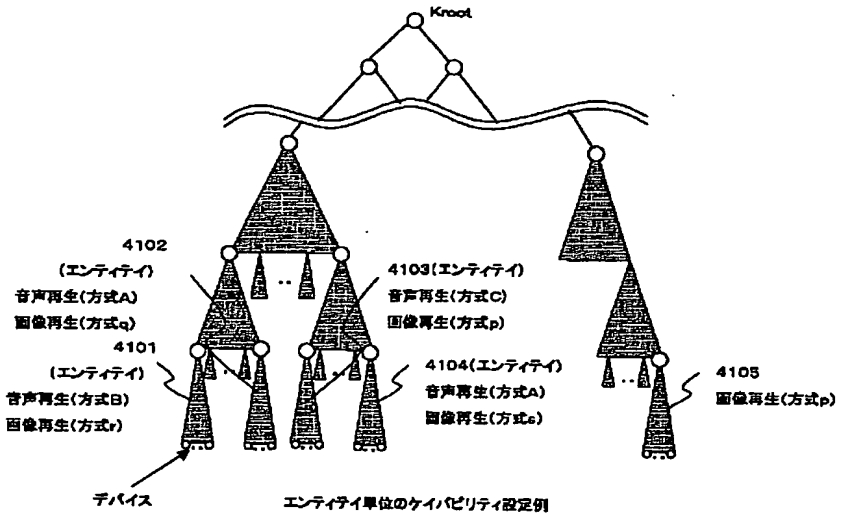


【図４０】



エンティティ単位のケイパビリティ設定例

【図４１】



【図４２】

(a)

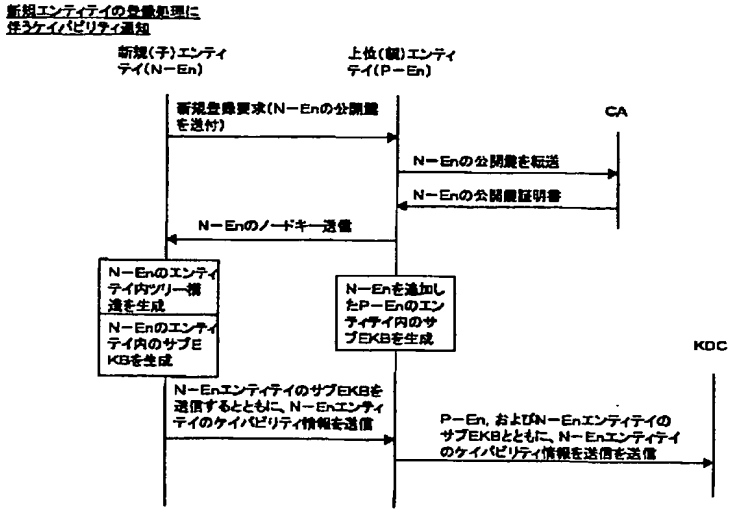
ケイパビリティ(Capability)リスト								エンティティID	EKB	サブルート
1	0	1	0	1	0	1	0	Ent0010	EKB0010	K0010
0	0	1	0	0	0	1	0	Ent0011	EKB0110	K0110
1	1	1	1	1	0	0	0	Ent0012	EKB0011	K0011
:	:	:	:	:	:	:	:	:	:	:
0	0	1	1	1	0	1	1	Ent00nn	EKB00nn	K00nn

(b)

ケイパビリティ(Capability)リスト							
1	0	1	0	1	0	1	0

音声データ再生処理(方式A)(Yes:1, No:0)
音声データ再生処理(方式B)(Yes:1, No:0)
画像データ再生処理(方式C)(Yes:1, No:0)
画像データ再生処理(方式D)(Yes:1, No:0)
音声データ記録処理(方式M)(Yes:1, No:0)
:

【図４４】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	
			６０１Ａ	

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA03 BA07 CA15 CA16
5B082 EA11
5B085 AA08 AE29
5B089 GB03 JA33 JB22 KA08 KA17 KC20 KH30
5J104 AA01 AA16 EA02 EA04 EA06 EA17 MA05 NA02 NA03 PA10

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☒ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.